

19

Weltall zu klein?

$4 \cdot 10^{18}$, das sagt sich so leicht, ist auch schnell hingeschrieben, beansprucht nur wenige Zeichen, täuscht vor, kürzer zu sein, aber was, wenn man so ein Lineal kaufen möchte, nicht 30 cm lang, sondern $4 \cdot 10^{18}$? Oder, schon ein wenig eindrucksvoller in der Darstellung, 4000000000000000000?

1 Zentimeter für jede natürliche Zahl, und Oliveira e Silvas Verifikation reicht 4,23 Lichtjahre weit, das ist ziemlich genau bis zum nächsten Fixstern Proxima Centauri (4,27 Lj Entfernung). Wie könnte dann eine Leiter aussehen, wenn selbst das Licht von Sprosse zu Sprosse durchaus vier Jahre unterwegs sein darf?

2013 beschreiben Harald Andrés Helfgott – der peruanisch-französische Mathematiker, ein echter Kosmopolit und in vielen Sprachen zu Hause, forscht zu dieser Zeit an der École Normale Supérieure in Paris – und David J. Platt vom Heilbronn Institut der Universität Bristol die Durchführung so eines Leiterkonstruktionsverfahrens, das sie auf Basis von Oliveira e Silvas Verifizierungsdaten entworfen haben. Dabei geht es, im Stil von Saouter, eine Folge von Primzahlensprossen hinauf, die die Richtigkeit der ternären Goldbachschen Vermutung bis $8,875 \cdot 10^{30}$ bestätigen soll. Genauer, aber nicht vorstellbarer: bis 8875694145621773516800000000000. Ein Lineal der Länge 8875694145621773516800000000000 cm würde über 9000 Milliarden Lichtjahre weit reichen. Kein wirklich anschaulicher Vergleich, fällt eher unter den Tatbestand der Zahlenprotzerei, denn dafür müsste selbst das für uns beobachtbare Weltall – Spekulationen über alles andere an dieser Stelle mit voller Absicht aus-

geblendet – mit seinen geschätzten ca. 93 Milliarden Lj Durchmesser noch ein wenig expandieren. Was natürlich dauert. Eine ebenso lange Wäscheleine könnte man immerhin aufrollen. Ungeknickt und unzersägt, passt so ein Maßstab momentan auf keinen Fall da rein.

Gute Idee deshalb von Helfgott und Platt, solch eine monströse Strecke zur Primzahlensuche erst einmal in 492700 handliche Abschnitte zu zerlegen. Dann erstreckt sich ein einzelnes Teilstück, wenn man pro natürlicher Zahl wie gehabt 1 cm ansetzt, nur noch 19 Millionen Lichtjahre weit, das ist schon besser zu überblicken, wenn auch noch neunmal bis zum Andromedanebel. Aber der ist ja auch eine Nachbargalaxie.

Jedes der 492700 Teilintervalle, $1,8 \cdot 10^{25}$ natürliche Zahlen umfassend, wird anschließend separat ausspioniert. Um Zeit zu sparen, stehen dabei aber stets mehrere gleichzeitig unter Beobachtung. Diese parallele Vorgehensweise, samt gewählter Intervallgröße, ist optimal auf die von Helfgott und Platt benutzten Rechner abgestimmt, denen eine Multi-Core-Prozessorarchitektur atemberaubende Dynamik verleiht (hier hinter werbewirksamer Wortwahl versteckt: drei Computercluster an zwei verschiedenen Standorten, davon einer mit insgesamt 48 Prozessorkernen).

Für so ein intergalaktisches Teilintervall braucht man – bei einem zulässigen Sprossenabstand bis kurz vor Proxima Centauri – mindestens, π mal Daumen, 4,5 Millionen Primzahlen. Außerdem ist bei der Konstruktion einer Leiter innerhalb des jeweils zu durchfilzenden Abschnitts zusätzlich sicherzustellen, dass der erlaubte Maximalabstand der Primzahlen auch beim Verschweißen der Einzelstücke zur lückenlosen Gesamtstrecke niemals überschritten wird. Vorsicht also jeweils an Anfang und Ende. Insgesamt sind für die ganze 887569414562177351680000000000er-Strecke

nicht weniger als großzügige 2,2 Billionen ($2,2 \cdot 10^{12}$) unzerbrechliche Querlatten einzusetzen. Deren Qualität ist natürlich strengstens zu überprüfen.

Es ist deshalb von Vorteil, wieder Primzahlverdächtige einer sehr speziellen Bauart heranzuziehen, die einfacher zu inspizieren sind. Helfgott und Platt entscheiden sich hier für sogenannte Proth-Zahlen. Vor dem entsprechenden Spezialcheck wird aber, genau wie bei Saouter, ein Sieb vorgeschaltet, nur diesmal feiner, um die Teilbarkeit der in Frage kommenden Kandidatinnen durch alle Primzahlen kleiner als 16000 zu überprüfen. Nach wie vor eine Kompromisslösung, was die Rechenzeit betrifft, auch wenn die Geräte seit Saouters Leiteralgorithmus von 1996 natürlich erheblich an Geschwindigkeit zugelegt haben.

Der Primzahltest selbst beansprucht nur ein klein wenig mehr kWh als eine kurze Pause im Screensavermodus. Deshalb, falls gewünscht, jetzt einfach auf eine etwas höhere Auflösung des Sachverhalts umschalten:

Proth-Zahlen sind nach dem mathematischen Autodidakten und Landwirt François Proth (1852–1879), der in der Nähe von Verdun lebte, benannt. Helfgott und Platt definieren sie als Zahlen der Form $N = k \cdot 2^n + 1$,

wobei k und n natürliche Zahlen größer als 0 darstellen; zusätzlich muss k ungerade und kleiner als $2n$ sein. Prothsche Primzahlen genügen diesen Anforderungen, sind aber zusätzlich prim (zum Vergleich: Saouters Primzahlsprossenschema lautet $N = k \cdot 5 \cdot 223 + 12582913$).

Die kleinste Zahl Proth-Zahl 3, mit $k = 1$ und $n = 1$ ($1 \cdot 2^1 + 1 = 3$, es gilt $1 < 2^1$) ist gleichzeitig auch die kleinste Prothsche Primzahl. Zu seinen

Zahlen hat François Proth gleich vier „Theoreme“ (Sätze) mitgeliefert, wovon eines hier als relativ einfacher Primzahltest benutzt werden soll:

Ein Blick, sozusagen ins Erdinnere einer Proth-Zahl, ganz ohne Kenntnisse in Festkörper- oder Geophysik, man braucht dazu weder Druck- noch Temperaturverhältnisse, wie sie im Zentrum des blauen Planeten herrschen, zu simulieren.

Auch das kein Ding der Unmöglichkeit übrigen, eine spezielle Apparatur erlaubt es sogar, das Verhalten millimeterkleiner Gesteinssplitter unter Bedingungen, wie sie im Erdkern herrschen, direkt zu beobachten. Eingeschlossen in eine winzige, fies aufheizbare Kammer, sozusagen lupenrein in der mehrere-Millionen-bar-Klemme zwischen zwei durchsichtigen Druckstempeln, für die nur ein einziges Material in Frage kommen kann: Diamant.

Zu edle Sache für den größeren Maßstab, aber um voluminöse Proth-Zahlen in die Zange zu nehmen, braucht man zum Glück kein hochkarätiges Equipment, sondern nur günstige Zahlenanalytik. Die beginnt, wie so oft, mit Ausprobieren, schön der Reihe nach. Damit ein optimales Einsatzfeld für Computer – ganz ohne zusätzliche Diamantstempelzellen-Hardware-Ausrüstung:

Zunächst braucht dazu nämlich nur, passend zum Proth'schen Versuchsobjekt N , eine weitere natürliche Zahl a gesucht werden, die eine bestimmte Bedingung erfüllt. Soweit die erfreuliche Mitteilung. Und wer an dieser Stelle neugierig werden möchte, bitte schön, jetzt kommt – und das ist die schlechte Nachricht – ein Häppchen sehr ausgefallenes Futter: Dieses

a ist so auszuwählen, dass eine gewisse gemeine Heimsuchung von Rechenoperation damit, nämlich die Bestimmung des sogenannten „Jacobi-Symbols“, den Wert -1 liefert. Eine kleine Anleitung, die genau das vorführt, findet sich zum Beispiel im Prime Glossary von Chris K. Caldwell. Das muss man nicht unbedingt schlucken. Hat vermutlich, genau wie die brillanten Druckstempel, Härte 10. Feuerquasarwinkel, die Fluoreszenzflächen brechen, scharfkantige Spektralsplitter. Geht auch ohne weiter im Text.

Nun kann man, auch bei enormer Rechenleistung, nicht für jede Proth-Zahl alles Denkbare durchprobieren. Helfgott und Platt entscheiden sich deshalb, für a nacheinander nur die ersten zehn Primzahlen (2, 3, 5, 7, 11, 13, 17, 19, 23, 29) einzusetzen, selbstverständlich mit hinterhältigem Plan in petto: Jede ist mit immerhin fünfzigprozentiger Wahrscheinlichkeit ein Treffer; daraus folgt, dass sich in maximal zehn Versuchen damit für 99,9 % aller Proth'schen Probandinnen ein geeignetes a finden lässt. Sollte es wider Erwarten nichts Passendes innerhalb dieser Kollektion geben, wird abgebrochen, der Proth-Zahl (durchaus auch fälschlicherweise, was in diesem Zusammenhang aber nicht schlimm ist) das Etikett „keine Primzahl“ aufgeklebt und die nächste untersucht. Normalerweise sind nämlich genug davon da – an die 4 Milliarden drängeln sich in jedem der 492700 Teilabschnitte, also durchschnittlich 888 Stück pro $4 \cdot 10^{18}$ - Strecke.

Sobald aber für eine zu testende Zahl N ein geeignetes a festgesetzt werden kann, startet die eigentliche Prüfung. Dabei spielt Teilbarkeit eine wichtige Rolle – und im, auch diesmal wieder

völlig freiwilligen Nerd-Buffer lautet diese Aussage dann so: $a^{(N-1)/2} + 1$ muss durch N teilbar sein, es darf kein Rest bleiben (oder, noch schlimmere Schreibweise, ganz ohne Formeleditor, aber mit identischer Aussage: $a^{(N-1)/2} \equiv -1 \pmod{N}$). Auch das können die Gehirnstromkurven im Rahmen eines Pilotprojekts gerne weiträumig umfließen, wichtig ist nur: Besteht die Proth-Zahl, ist sie prim. Mit hundertprozentiger Sicherheit. Das ist ein großer Vorzug dieses Verfahrens.

In seltenen Fällen kann es aber passieren, dass sich so keine Proth-Zahl in passendem Abstand als prim entlarven lässt, trotz hunderter Verdachtsfälle. Dann braucht man einen Plan B, um eine ganz allgemeine Primzahl zu finden – die wachsen in diesen Bereichen ja noch dicht genug, wie das Unternehmen Antarktistouristik gezeigt hat. Oder besser gleich: einen Plan *PARI/GP*.

Die Abteilung für Kryptologie findet heraus, das es sich bei dieser Buchstaben-/Zeichenkombination um den Namen eines frei zugänglichen Computeralgebra-systems handelt. Es bietet unter anderem auch effiziente Funktionen, die mutmaßliche Primzahlen (sog. „Pseudoprimzahlen“) gewünschter Größenordnung fabrizieren und auf Echtheit überprüfen können, an. Das dauert selbstverständlich länger als die von Proth inspirierte Suche, ist aber bei nicht ganz so vielen angeforderten Zahlen gerade noch zeitlich verträglich – was nach einem schon stark angespannten Geduldsfaden klingt und erneut jahrhundertelange Prozessorquälerei befürchten lässt. Dabei beansprucht die Leiterkonstruktion innerhalb eines $1,8 \cdot 10^{25}$ - Intervalls gerade mal rund 270 Sekunden! Nur viereinhalb Minuten, einschließlich des vorgeschalteten Siebvorgangs und der Suche allgemeiner Primzahlen mit Hilfe von *PARI*-Funktionen. Diese brauchen, in allen 492700 Abschnitten, lediglich in 130917 Fällen einzugreifen.

Und da man niemals einer einzelnen Programmausführung trauen sollte, wird der Sondertest für sämtliche Prothschen Primzahlen wiederholt, die Korrektheit der dazwischen liegenden Abstände ebenfalls noch einmal überprüft, alles aber diesmal auf anderer Softwaregrundlage. 40 Sekunden dauert das zusätzlich, insgesamt kommen so gut 5 Minuten pro Abschnitt zusammen. Wobei hier allerdings bei keiner einzigen Berechnung Abweichungen oder offensichtliche Fehler auftreten.

Auch die von *PARI* gelieferten Primzahlen müssen einem zweiten Spaltungsversuch widerstehen. Hier kommt das bereits bekannte Programm *Elliptic Curve Primality Proving* zum Einsatz, der Zeitaufwand im *ECPP*-Reaktor wird gar nicht erwähnt, da kaum der Rede wert. Ebenfalls niemals irgendwelche Diskrepanzen, lautet das Ergebnis.

Alles in allem für fast eine halbe Million Abschnitte durchgeführt, dauert dann doch etwas länger: Gut 40000 Stunden (über 4,5 Jahre) Rechenzeit kommen so für die gesamte Verifikation letztendlich zusammen, parallel verteilt auf sämtliche Prozessoreinheiten aller drei Computercluster, in Realzeit damit wesentlich weniger.

Würde man diese Verifikation „nur“ bis 10^{27} durchführen, fiel das, so Helfgott, „noch gut in den Bereich des Home-Computings“. Bedeutet: Je nach Leistung des haushaltsüblichen Rechners ist hier von 5 bis 25 h Laufzeit auszugehen, nicht mehr als eine kleine Aufgabe „fürs Wochenende“, aber ein großes Plus für die Überprüfbarkeit. Dabei wäre diese Reichweite schon sehr, sehr ordentlich – 10^{27} cm entsprechen immerhin 1 Milliarde Lichtjahren!

Da für die gesamte, fast 9000 mal so lange Verifikation das Universum immer noch ein paar Zentimeter zu

kurz geraten ist, obwohl es sich in den letzten Minuten erheblich ausgedehnt hat, soll deshalb jetzt versuchsweise der atomare Goldstandard zu Rate gezogen werden. Wobei das Edelmetall seinen astronomischen Ursprung schlecht verleugnen kann – als ehemaliger Sternenstaub, durch Supernova-Explosionen entstanden und verteilt. Statt als flaches Blattgold zu enden, wird es diesmal zu einer atomar dünnen Kette, bei der die Atome wie auf einer Perlenschnur aufgereiht sind, langgezogen. Das ist gar nicht so unrealistisch und in extremen Größenordnungen viel handlicher als ein cm-Lineal: Legt man dabei den üblichen Abstand der Au-Atome im Metallgitter zugrunde, ergeben rund $4 \cdot 10^{18}$ Stück davon eine Kettenlänge, die fast drei Mal bis zum Mond reicht. Dabei bringt diese Menge nur ganze 1,3 mg auf die Waage, ein winziger Goldfitter und durchaus erschwinglich von den Materialkosten her. Eines der 492700 Teilintervalle würde in solcher Form dann aber schon ein halbes Lichtjahr weit reichen, bei einer Masse von stolzen 5,9 kg durchaus im höherpreisigen Segment anzusiedeln, aber noch gut zu tragen. Deshalb auch nach Fertigstellung des letzten Satzes nicht mehr gesehen. Die Version für zuhause, 10^{27} Einzelatome, garantiert nicht aus Katzensgold gesponnen, zieht mit 30 Lichtjahren Schnurlänge und grazilen 327 kg großzügig an der Wega vorbei. Helfgott und Platts gesamte Kette von $8.875 \cdot 10^{30}$ zusammengehäkelten Einheiten umfasst hingegen 270000 Lichtjahre und lässt sich locker mehr als zweieinhalbmals über das ganze Milchstraßensystem spannen. Das Weltall sprengt sie so nicht mehr, dafür aber das Budget – über 2900 Tonnen Gold stecken drin!

Wie Sie in Ihrem aufgeklärten Skeptizismus vielleicht bereits bemerkt haben, hatte soeben schon wieder die Astronomie die Kontrolle über die Autorin übernommen, über sehr weite Strecken sogar. Es scheint kaum möglich, dieses Gebiet dauerhaft abzuschütteln, gerade im Umfeld großer Zahlen. Wir arbeiten aber daran.

Die Zukunftsperspektive hingegen ist schon fertig und ein Weitermachen durchaus möglich: Theoretisch könnte man mit dem Verfahren von Helfgott und Platt sogar bis $2 \cdot 10^{31}$ kommen, danach dünnen die Proth-Zahlen zu sehr aus, ungefähr auf halbe Dichte, was zur Folge hätte, dass wesentlich mehr allgemeine Primzahlen mit Hilfe von *PARI* gesucht werden müssten. Der Zeitbedarf würde dadurch wesentlich steigen. Ob sich das in diesem Fall lohnt?

Eine Entscheidung verschiebt sich auf später, ganz von allein.

Und wird vom etwas sehr Wichtigem überblendet. Denn nach wie vor gibt es da so eine Sache, der alles Verifizieren nichts anhaben kann.