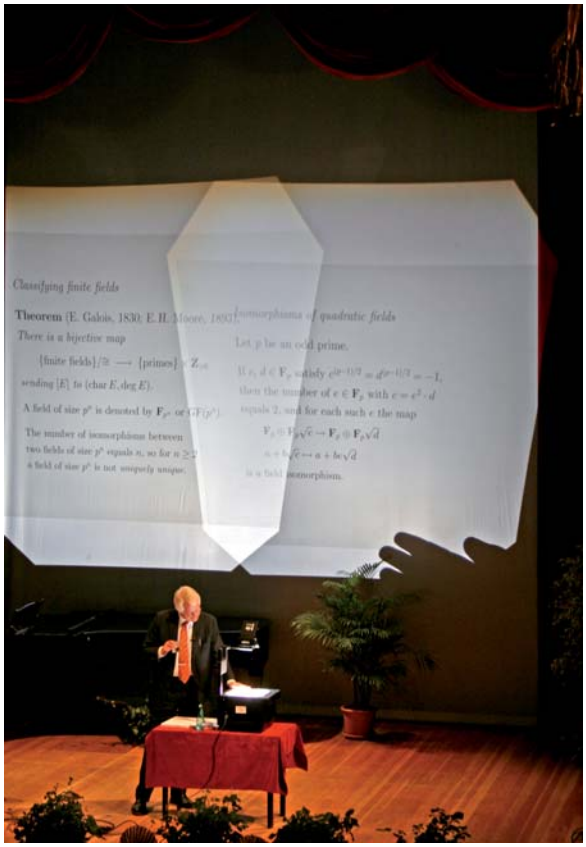
„Mathematik ist mein Leben“

Ein Gespräch mit Hendrik W. Lenstra



Hendrik W. Lenstra hält die Euler-Vorlesung 2009 (Foto: Thomas Vogt)

Hendrik W. Lenstra, Jahrgang 1949, ist ein niederländischer Zahlentheoretiker, der unter anderem mit seinen Arbeiten zu Faktorisierungsalgorithmen berühmt wurde. Auch zwei seiner Brüder sind bekannte Mathematiker. Lenstra hat aber nicht nur Mathematik im Kopf. Seit seiner Kindheit spielen auch die griechische Sprache und Literatur eine wichtige Rolle in seinem Leben. Gedichte aus der Griechischen Anthologie und die Epen Homers liest Lenstra am liebsten im Original.[1] *Eine weitere Liebe Lenstras gilt der Kunst, insbesondere den Werken des niederländischen Künstlers und Grafikers M. C. Escher. Als er vor einigen Jahren für Eschers Lithografie* Prententoonstelling *(Bildergalerie) mit mathematischen Methoden die Fortsetzung der Bildergalerie im Zentrum des Bildes konstruierte, wurde er einer breiteren Öffentlichkeit bekannt.*[2] *Lenstra wird am 30. Oktober 2009 um 16 Uhr im Krönungssaal des Rathauses in Aachen die 15. Gauß-Vorlesung der DMV halten (s. S. 74). Der Titel der Gauß-Vorlesung lautet „Modelling finite fields“. Mit dem Zahlentheoretiker sprachen am Rande der Euler-Vorlesung am 29. Mai 2009 in Potsdam der Herausgeber der* Mitteilungen, *Martin Skutella, und Thomas Vogt vom Medienbüro der DMV.*

Bitte erzählen Sie uns, wie Sie zur Mathematik gekommen sind.

Das weiß ich nicht. Als ich 6 oder 7 Jahre alt war, fragte unsere Lehrerin einmal die Schülerinnen und Schüler, was sie später werden wollten. Die meisten haben gesagt: Polizeibeamter, Pilot oder Mannequin. Und ich habe gesagt „Professor der Mathematik“. Da haben alle gelacht, aber ich war wohl der Einzige, der Recht behalten sollte.

Wie kam es zu dieser Aussage?

Ich denke, dass da zwei Dinge zusammenkamen. Zum einen war mein Vater Mathematiklehrer. Zum anderen war ich nicht sehr gut in Sport und schon gar nicht bei Raufereien. Aber es gab da eine Sache, in der ich richtig gut war: Zahlen und logisches Denken. Und es war ganz klar, dass das meine Erfolgsformel sein würde.

Auch zwei Ihrer Brüder sind bekannte Mathematiker.

Ja, ich habe vier Brüder und eine Schwester. Unser Vater hat uns bei Tisch immer mathematische Rätsel gestellt, und wir Brüder konkurrierten dann bei der Lösung. Meine Schwester war weniger enthusiastisch, was Mathematik anbelangt.

Gemeinsam mit Ihrem Bruder Arjen Lenstra und mit László Lovász haben Sie den sogenanten LLL-Algorithmus zur Gitterbasisreduktion entwickelt. Wie ist das, wenn man mit seinem Bruder zusammen arbeitet?

Das ist interessant, dass Sie das fragen. Mein Bruder Arjen ist 7 Jahre jünger als ich. Als er noch an seinem Diplom oder an seiner Doktorarbeit arbeitete, war ich bereits Professor. Er interessierte sich eher für praktische Dinge, war in der Informatik und ich in der Mathematik. Wenn er ein theoretisches Problem hatte, fragte er mich manchmal um Rat. Wir teilten uns damals eine Wohnung, sprachen aber nicht viel über Fachliches.

Wie kam es dann zu LLL?

Lassen Sie mich die folgende Geschichte erzählen: Vor zwei Jahren gab es eine Konferenz in Caen, in der Normandie. Die hieß „LLL + 25“, weil 1982 der LLL-Artikel publiziert worden war. Der erste Morgen der Konferenz war der Entstehungsgeschichte gewidmet, und jeder der drei L hat seine eigene Version der Geschichte erzählt.

Thomas Vogt (li.) und Hendrik W. Lenstra (Foto: Martin Skutella)

Und da habe ich von meinem Bruder zum ersten Mal erfahren, wie er die Sache erlebt hat. Und das war ganz anders, als ich sie erlebt hatte. Lovász und ich haben ungefähr das Gleiche gemacht. Aber mein Bruder hat Sachen mit Hilfe numerischer Experimente entdeckt.

Mein Bruder beschäftigte sich damals mit der Entwicklung und dem Implementieren von Algorithmen zum Faktorisieren von Polynomen. Dabei stieß er auf ein bestimmtes Problem und fragte mich um Rat. Ich erklärte ihm, wie er sein Problem mit Hilfe einer damals noch primitiven Form der Gitterbasisreduktion lösen konnte. Etwa ein halbes Jahr später bin ich zu einem Vortrag von ihm gegangen, bei dem er die Idee in wesentlichen Teilen geändert hatte. Er hatte die Technik, die ich ihm vermittelt hatte, auf eine ganz andere Weise angewendet. Ich habe es sehr bewundert, wie er das gemacht hat. Erst später, in Caen, habe ich gehört, was geschehen war: Er hatte in seinem Programm einen Fehler. Er wollte etwas ausrechnen, hat aber $n + 1$ statt n gewählt. Dann hat der Algorithmus etwas für ihn völlig Überraschendes ausgegeben. Das sind die Fehler, die zu Entdeckungen führen!

Arbeiten Sie auch mit Computerexperimenten?

Nein, das ist nicht mein Stil. Ich interessiere mich zwar sehr für Algorithmen, aber aus rein theoretischer Sicht. Eigentlich ist das für einen Mathematiker eher ungewöhnlich. Also wenn man einem theoretischen Informatiker begegnet, dann ist er häufig ausschließlich an der Theorie, der Komplexität der Algorithmen interessiert; aber die Mathematiker interessieren sich oft viel stärker dafür, mit Algorithmen etwas praktisch zu berechnen. Nehmen Sie zum Beispiel die Computer-Algebra. Da werden nicht so viele Sätze bewiesen. Also „2 mal 3 ist gleich 6“ ist kein Satz, aber es macht einen Unterschied, wenn wir stattdessen „6 ist gleich 2 mal 3“ schreiben und uns dabei vorstellen, dass die Zahl 6 gegeben war und uns fragen, wie man die 2 und die 3 gefunden hat. Das Problem des Faktorisierens, also die Primfaktoren einer gegebenen Zahl zu ermitteln, ist eine spannende Herausforderung. Es wurde viel Energie investiert, für die Praxis einsetzbare Algorithmen zu entwerfen und damit konkrete Beispiele zu lösen. Aber Mathematiker sollten Sätze beweisen und nicht nur Beispiele rechnen. Sie sollten Aussagen dazu treffen, was ihr Algorithmus leisten kann. Und diese Aussagen sollten allgemein sein, also für unendlich viele Fälle gelten.

Wie arbeiten Zahlentheoretiker? Wie dürfen wir uns die Forschung in Ihrer Arbeitsgruppe vorstellen?

Meine Arbeitsweise hing sehr davon ab, auf welcher Stufe meiner Karriere ich gerade war. Als Student habe ich viel allein gearbeitet. Ich habe sozusagen zehn Jahre in der Bibliothek gewohnt, umgeben von Büchern; das war die Luft, die ich geatmet habe, all die Mathematik. Das war nicht einsam; man war zwar oft allein, aber tagsüber waren da ja die anderen Studenten und die Professoren. Später, wenn man Karriere gemacht hat, kann man das nicht mehr machen. Und wenn Sie fragen, wie ich heute arbeite: Heute arbeite ich nicht mehr (lacht) – ich beantworte meine E-Mails. Wenn ich mathematische Ideen habe, dann gehe ich zu meinen Studenten und steuere die Arbeit an diesem oder jenem Problem. Es gibt viele Dinge, über die nachzudenken ich noch keine Zeit gehabt habe. Aber in vier oder fünf Jahren werde ich emeritiert sein, und dann habe ich hoffentlich wieder Zeit dafür, selbst Probleme zu lösen und zu publizieren.

Sie haben lange in Berkeley gearbeitet, sind aber vor etwa zehn Jahren in die Niederlande zurückgekehrt. Wie unterscheidet sich die Arbeit in den USA von der in Holland?

In Berkeley hat niemand Zeit. Wenn man eine Frage hat, dann geht man nicht in das Büro eines Kollegen, sondern schreibt ihm eine E-Mail. Die Amerikaner arbeiten sehr hart. In Leiden stehen unsere Türen immer offen, und die Leute kommen rein, wenn sie Fragen haben. Ich fühle mich in Leiden viel verantwortlicher dafür, wie die Sachen laufen, als ich es in Berkeley getan habe. Weil Berkeley so groß ist; und ich war natürlich nicht der Einzige. In Berkeley hätte ich jede Stunde zu einem interessanten Vortrag gehen und nichts anderes machen können.

Und in Leiden?

Im ersten Jahr war niemand da. Man hätte in der Halle eine Kanone abfeuern können, und niemand hätte es gehört. Ich musste alles von Grund auf aufbauen.

Wie sehen Sie das Verhältnis zwischen Reiner und Angewandter Mathematik?

Da gibt es viele Klischees, und viele davon haben auch einen wahren Kern. Ich würde eher von verschiedenen Stilen in der Mathematik sprechen. Und kein Stil ist besser als der andere, letztendlich brauchen wir alle. Die Probleme in der Mathematik sind so gewaltig, dass wir jeden einzelnen Ansatz brauchen, um sie zu lösen.

Als ich Student war, zerfiel die Mathematik für mich in zwei Hälften: den diskreten Teil und den kontinuierlichen Teil. Zum diskreten Teil gehörten Algebra, Gruppentheorie, Logik und Mengenlehre. Dann gab es da die Kontinuierliche Mathematik, also alles Geometrische, die Analysis, Differentialgleichungen etc. Heute weiß ich, dass es da viele Verbindungen gibt. Aber als Student war ich

der Meinung, dass nur die Diskrete Mathematik vollkommen und von Menschenhand geschaffen war. Ich konnte mich darin allein und frei bewegen, brauchte niemanden sonst, konnte nachdenken und entscheiden, ob Dinge wahr oder falsch sind. Natürlich gab es unentscheidbare Probleme – das wusste ich. Aber prinzipiell gilt für die allermeisten Probleme, denen man in der Diskreten Mathematik begegnet: Man beweist sie oder findet ein Gegenbeispiel.

Und wie sahen Sie den kontinuierlichen Teil der Mathematik?

Also ich war jung – und ich weiß nicht, ob das mein eigenes Versäumnis war oder an der Art und Weise lag, wie es mir vermittelt wurde – jedenfalls hatte ich den Eindruck, dass es sich dabei nicht um axiomatische Mathematik handelt. Mir schien es, als ob die Leute dort versuchten, die reale Welt mit Definitionen einzufangen; sozusagen das zu beschreiben, was man als wahr erkannt hatte.

Was ist ein Axiom? Für die Griechen war ein Axiom etwas Wahres, das keiner Erklärung bedurfte. Doch für die moderne Mathematik ist ein Axiom lediglich eine Hypothese. Die Analysis und sogar die Lineare Algebra schienen damals für mich auf dem axiomatischen Verständnis der Griechen zu beruhen. Und so hatte ich das Gefühl, dass ich es bei der Beschäftigung mit Analysis und Linearer Algebra mit der realen Welt zu tun bekam. Und die reale Welt war zu schwierig für mich.

Wann änderte sich Ihr mathematisches Weltbild?

Ich glaube, es war in meinem ersten oder zweiten Studienjahr, als wir Körpererweiterungen behandelt haben. Da gibt es den Begriff des Grades einer Körpererweiterung, der mit Hilfe der Linearen Algebra definiert wird. Aber die Lineare Algebra gehörte für mich in die andere Hälfte der Mathematik. Ich dachte, das kann man doch nicht machen! Man kann doch nicht physische Begriffe auf diskrete anwenden! Und dann habe ich mir die Lineare Algebra genauer angeschaut und habe verstanden, dass auch sie sauber axiomatisch aufgebaut ist. Also habe ich in meinem Geiste die Lineare Algebra von der Kontinuierlichen in die Diskrete Mathematik verpflanzt - und damit war das Problem für mich gelöst.

Heute denke ich natürlich ganz anders darüber. Leider arbeiten auf der Schnittstelle zwischen der Diskreten und Kontinuierlichen Mathematik verhältnismäßig wenige Mathematiker, dabei bräuchten wir sie dringend.

Gibt es Anwendungsgebiete für Ihre theoretischen Arbeiten?

Ja, für den LLL-Algorithmus zum Beispiel. Ich kenne zwar keine Details, aber man hat mir erzählt, dass LLL zum Beispiel eine wichtige Rolle bei der Entfernungsmessung via Satellit spielt und damit von zentraler Bedeutung für das GPS ist. Und natürlich gibt es viele Anwendungen von LLL in der Kombinatorischen und Ganzzahligen Optimierung.

Martin Skutella (li.) und Hendrik W. Lenstra (Foto: Thomas Vogt)

Sie haben auch den Zusammenhang zwischen elliptischen Kurven und dem Faktorisieren von Zahlen entdeckt.

Ja, das war in den frühen 80er Jahren. Ich arbeitete nicht in der Algebraischen Geometrie, das war mir zu geometrisch. Mein Betreuer während des Studiums in den 70er Jahren war ein Algebraischer Geometer. Aber ich habe Algebraische Geometrie nie so richtig gelernt. Dafür habe ich ihm Algebraische Zahlentheorie beigebracht. Es war zu dieser Zeit noch nicht so klar, dass die Algebraische Geometrie sehr wichtige Anwendungen in der Algebraischen Zahlentheorie hat.

Wie haben Sie dann diesen Zusammenhang hergestellt?

Es gab da den Beweis der sogenannten Hauptvermutung in der Theorie der Kreisteilungskörper. Das sind Zahlkörper, die man durch Adjungieren von Einheitswurzeln erhält. Es gab Vermutungen, und Leute aus der Algebraischen Geometrie haben sie bewiesen. Damit war klar, dass man als Zahlentheoretiker doch Algebraische Geometrie lernen sollte. Und dann hatte ich einen ehrgeizigen Studenten, René Schoof, der sich intensiv mit elliptischen Kurven befasst hat. Er hat mich elliptische Kurven gelehrt, so wie ich meinen Betreuer Algebraische Zahlentheorie gelehrt hatte. Und dann lag der Zusammenhang plötzlich auf der Hand. Ich hatte mich bereits mit diesen Algorithmen beschäftigt und habe dann auf einmal gesehen, dass die elliptischen Kurven eine Anwendung haben, nämlich das Faktorisieren.

Die Sicherheit vieler Kryptosysteme beruht auf der unbewiesenen Annahme, dass es schwierig sei, große Zahlen zu faktorisieren. Wie schwierig ist dieses Problem Ihrer Meinung nach wirklich?

Ich möchte dazu nur das Folgende sagen: Das übliche Argument, Faktorisieren sei schwierig, weil über Jahrhunderte kein effizientes Verfahren dafür gefunden wurde, ist sehr schwach. Da sollte man ehrlicher sein und fragen, wie viele Mathematiker sich bisher ernsthaft damit beschäftigt haben und wie lange. Nehmen wir zum Beispiel den Primzahltest, also das Problem zu entscheiden, ob eine gegebene Zahl eine Primzahl ist. Auch das galt als schwierig. In den 1970er Jahren versuchten viele, dieses Problem zu lösen – lange ohne Erfolg. Und dann gelang

es 2002 auf einmal, einen Algorithmus anzugeben, der das Problem beweisbar effizient löst.

Übrigens gefällt mir die Anwendung der Zahlentheorie im Sinne der Kryptologie in einem Punkt nicht: Die Anwendung basiert darauf, dass wir etwas nicht können, nämlich große Zahlen zu faktorisieren. Sollte das Problem gelöst werden, würde die Anwendung verschwinden. Das ist genau anders herum als es üblicherweise ist und sein sollte.

Wie viele Ihrer Schüler arbeiten bei der NSA?

Das kann ich aus dem Kopf nicht sagen. Mindestens einer arbeitet dort. Ein anderer, der dort gearbeitet hat, musste aufhören. Und wissen Sie, warum? Weil er eine Chinesin geheiratet hat! Das war der NSA offenbar nicht geheuer. Jetzt ist er wieder an der Universität. Jedenfalls kenne ich die genaue Anzahl nicht; sie ist jedoch um eins kleiner als noch vor zwei Jahren.

Die Lösung welches offenen mathematischen Problems würden Sie gerne kennen?

P vs. *NP*. Das mag eine erstaunliche Antwort für einen Reinen Mathematiker sein. In den 1970er Jahren habe ich durch meinen Bruder Jan Karel, der auf dem Gebiet der Kombinatorischen Optimierung arbeitete, das Problem *P* vs. *NP* kennengelernt. Und das war eine ganz tolle Sache. Das ist eines der größten offenen Probleme, dessen Lösung ein neues Forschungsgebiet eröffnen könnte. In der Theoretischen Informatik bewegt man sich auf recht dünnem Eis, und die Lösung von P vs. NP würde hier eine solide Basis schaffen. Ich bin zwar kein Informatiker, aber ich habe das Gefühl, dass wir von einer Lösung des Problems noch sehr weit entfernt sind.

Kann man die Theoretische Informatik als Zweig der Mathematik bezeichnen?

Absolut. Oft ist die Theoretische Informatik mathematischer als Mathematiker es sind.

Und wie steht es mit der Goldbachschen Vermutung oder der Riemannschen Vermutung?

In der Tat liegen mir die Goldbachsche Vermutung und die Riemannsche Vermutung fachlich näher. Aber die Anstrengungen zum Beweis der Goldbachsche Vermutung würde ich eher als eine Art Sport bezeichnen, nicht als etwas, das wir der Sache wegen wissen wollen. Selbst wenn sie gelöst würde – die Goldbachsche Vermutung hätte kaum Konsequenzen für das Fachgebiet. Das sieht bei der Riemannschen Vermutung allerdings völlig anders aus.

Welche großen offenen Probleme werden Ihrer Meinung nach in absehbarer Zeit gelöst werden?

Ich bin mir gar nicht sicher, ob Mathematiker dazu geeignet sind zu beurteilen, welches Problem demnächst gelöst wird und welches nicht. Hilbert sagte mal bei einem Vortrag, bezüglich der Riemannschen Vermutung seien große Fortschritte gemacht worden, und er erwarte, dass sie noch zu seinen Lebzeiten gelöst werde. Fermats letzter Satz sei sicherlich etwas schwieriger zu beweisen, aber irgendjemand im Raum werde das noch erleben. Die Frage nach der Transzendenz von $2^{\sqrt{2}}$ sei dermaßen schwierig, dass wohl niemand im Raum ihre Lösung erleben werde. Und ein Jahr später wurde eben dieses Problem gelöst; Fermats letzter Satz wurde erst kürzlich bewiesen und die Riemannsche Vermutung ist noch völlig offen. Es kam also genau umgekehrt. Es bleibt also auch in Zukunft spannend in der Mathematik.

Hendrik W. Lenstra (Foto: Thomas Vogt)

Herzlichen Dank für das Gespräch.

Anmerkungen

1. *Siehe dazu auch:* Porridge Pulleys and Pi. Two Mathematical Journeys, *MSRI, 2004, 28:30 minutes, ISBN 0-9639903-6-5.*
2. *Siehe dazu auch: Artful Mathematics: The Heritage of M. C. Escher, Notices of the AMS, vol. 50, no. 4, 2003, 446–457. www.ams.org/notices/200304/fea-escher.pdf*