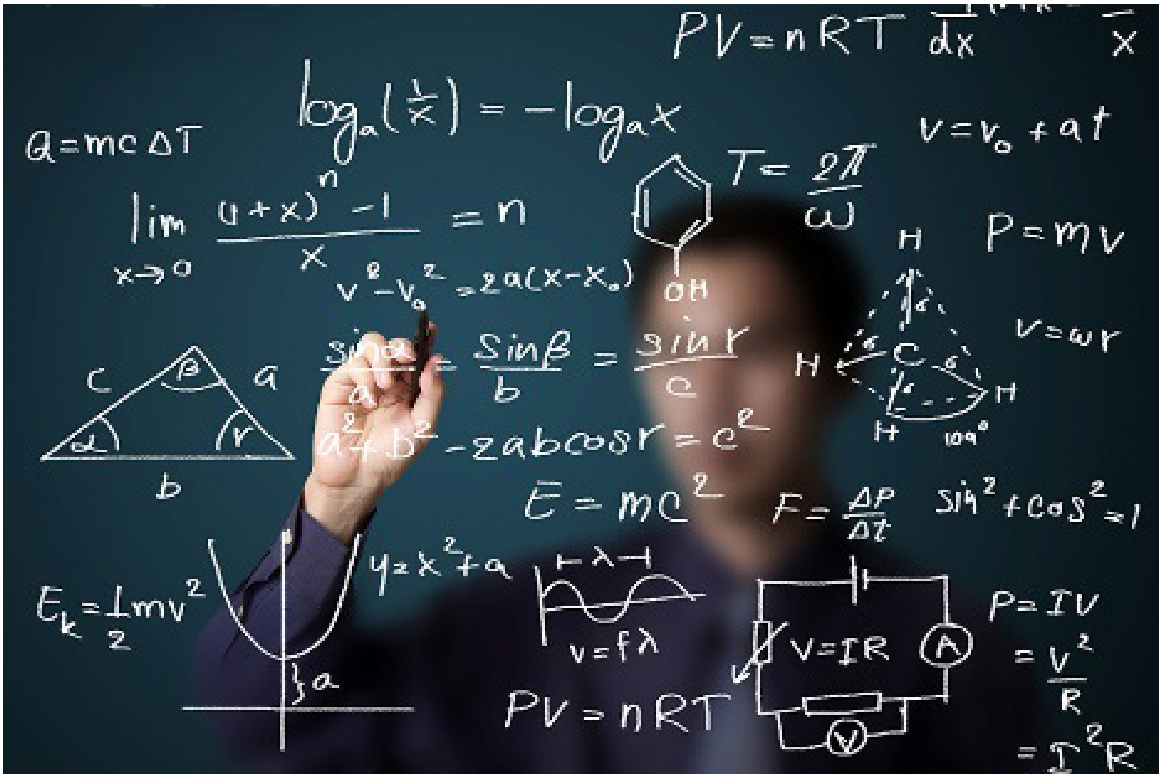
Beiträge des Humboldt-Clubs vom 24. November 2017

István GAÁL

STREIFZÜGE IN DER MATHEMATIK: VON DIOPHANTOS BIS ZU DEN HÖCHSTLEISTUNGSRECHNERN

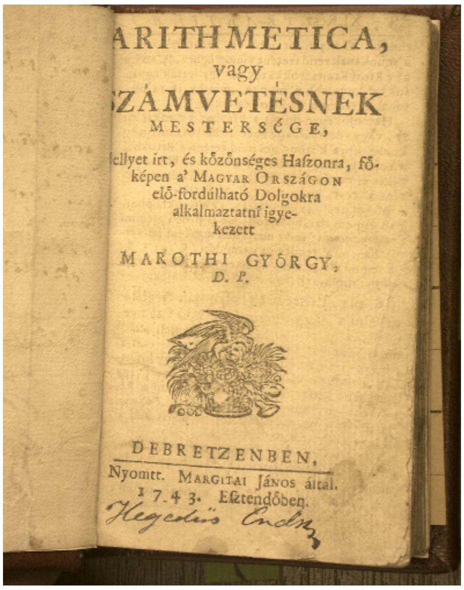


„*Was schon die alten Griechen wussten*“ – so beginnen alle Geschichten in der Mathematik. In der Tat hat bereits der große griechische Mathematiker *Diophantos* (zwischen 100 v. u. Z. und 350 v. u. Z.) interessante Probleme erörtert, die bis heute wichtig sind. Seine Gleichungen, die *diophantischen* Gleichungen, erhalten mehrere Variablen, die nur ganze Werte annehmen (z. B. –1, 0, 1, 2, 3 usw.). Er veröffentlichte seine Ergebnisse in 13 Bänden, was damals 13 Papyrusrollen bedeutete. Neun davon wurden im 15. Jahrhundert gefunden, weitere vier erst 1982. Eine seiner bekanntesten Gleichungen ist

(1) $x^2+y^2=z^2$

Ihre Lösungen sind die sogenannten *pythagoreischen* Tripel.

Das erste ungarischsprachige Buch über Arithmetik, verfasst von *György Maróti* im Jahre 1743, befindet sich in Debrecen, in der Bibliothek des Reformierten Kollegiums. Dabei stellt sich die Frage: Was machen eigentlich die heutigen Mathematiker?



ARITHMETICA,
vagy
SZÁMVETÉSNEK
MESTERSÉGE,
mellyet írt, és közönséges Haſzonra, fő-
képen a' MAGYAR ORSZÁGON
elő-fordúlható Dolgokra
alkalmaztatni igye-
kezett
MAROTHI GYÖRGY,
D. P.
DEBRETZENBEN,
Nyomtt. MARGITAI János által.
1 7. 4 3. Eſztendőben.

Ja, viele Mathematiker beschäftigen sich immer noch mit den *diophantischen* Gleichungen. Versuchen wir zum Beispiel, die folgende Gleichung zu lösen:

(2) $x^3-3x^2y-7xy^2-y^3=1$

Man sieht gleich, dass $(x,y)=(1,0),(0,-1)$ Lösungen sind, aber gibt es auch andere oder keine weiteren? Diese Gleichung hat zwar drei Grade statt zwei, wie in (1), hat aber nur zwei Unbekannte statt drei. Man dachte, dass es nicht viel schwieriger wäre, sie zu lösen. Das ist aber nicht der Fall. Alle *pythagoreischen* Tripel sind seit der Antike bekannt, die Lösung von (2) jedoch erst seit etwa 1970. Der norwegische Mathematiker *Axel Thue* hat 1909 bewiesen, dass die Gleichung (2) nur endlich viele Lösungen hat.

Das ist zwar schön, sagt aber gar nichts über die möglichen Lösungen aus. Ein ganz wichtiges Ergebnis hat der englische Mathematiker *Alan Baker* 1968 erreicht. Er hat eine explizite untere Schranke gegeben für bestimmte ganz allgemeine lineare Formen algebraischer Zahlen. *Baker* hat dafür die Fields-Medaille bekommen, den alternativen Nobelpreis für Mathematiker. Die erste Anwendung dieses Ergebnisses war eine obere Schranke für die Lösungen der Gleichungen ähnlich (2). Als Folgerung bekommt man eine explizit berechenbare Konstante *C*, so dass wir für alle ganzzahligen Lösungen *x,y* der Gleichung (2) Folgendes bekommen:

(3) max $(|x|,|y|)<C$.

Es war ein ganz großer Progress, weil es nur endlich viele ganze Zahlen mit Betrag kleiner als C gibt; man kann bei allen ausprobieren, ob sie eine Lösung sind oder nicht, und so kann man die tatsächlichen Lösungen auswählen. Damit hat man ein endliches Verfahren, einen „*Algorithmus*“, um die Lösungen zu finden.

Es klingt sehr schön. Das einzige Problem ist, dass C die Größenordnung exp() hat. Diese Zahl ist unheimlich groß, sie hat ca. 100000000000000000000 Ziffern. Zum Vergleich: Nach unseren Kenntnissen beträgt die Anzahl der Atome im Universum, die wir beobachten können, ca. , eine Zahl mit nur 80 Ziffern. Wir haben also keine Chance, alle ganzen Zahlen mit (3) auszuprobieren.

Dank *A. Baker* und *H. Davenport* (1969) gibt es ein Reduktionsverfahren, womit wir C sehr viel verringern können. Dafür berechnen wir eine Zahl T von den Koeffizienten der Gleichung (2). Um es einfach auszudrücken: zu T berechnet man eine ganze Zahl q, mit

(4) $|q|< 10^{22}$

und

(5) $||T^*q||<10^{-20}=0.0000000000000000000001$

und mit einer dritten Eigenschaft, was für uns hier nicht relevant ist (die Bedingung ist fast immer erfüllt). Hier ist $||x||$ die Entfernung von x zur nächsten ganzen Zahl (z. B. $||2.3||=0.3$, $||2.9||=0.1$). Die Zahl q zu berechnen bedeutet eine rationale Zahl p/q zu berechnen mit (4) so, dass es gilt:

$$\left|T-\frac{p}{q}\right|<\frac{10^{-20}}{q}$$

Diese Berechnung ist mit dem klassischen Kettenbruchalgorithmus ziemlich einfach. Die Zahl q findet man unter dem Nenner der Näherungsbrüche im Kettenbruchalgorithmus zu T.

$$\sqrt{2}=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{\ddots}}}}.$$

Die einzige Schwierigkeit ist, dass man hier mit ganz kleinen und ganz großen Zahlen rechnet, daher muss man T und alle anderen Zahlen mit der Genauigkeit von ca. 70 Ziffern berechnen. Das geht nicht mehr mit Taschenrechnern, dazu muss man ein allgemeines arithmetisches Programmpaket anwenden. Schauen wir uns an diesem Punkt ein konkretes Beispiel an:

T= 1.50203357738816300013503156419594795221191728122360058
q= 4412404287395170921
*T*q*= 6627579396679036676.9999999999999999999561183715

Die nächste ganze Zahl zu *T*q* ist *p*=6627579396679036677
||*T*q*||=|*q*θ-p*|= 0.000000000000000000043881679095952

Solche Berechnungen führen uns zu folgender Antwort: Die Gleichung (2) hat nur die trivialen Lösungen *(x,y)*=(1,0),(0,–1). Bei komplizierteren Gleichungen muss man natürlich ähnlich explizite Berechnungen durchführen, mit Zahlen von 1000 bis 2000 Ziffern. Bei anderen *diophantischen* Problemen ist es nötig, komplizierte algebraische Formeln in ein Produkt umzuwandeln. Gleichungen dieser Art zu lösen geht mit einem sehr großen Rechenaufwand einher. Um die Gleichungen zu lösen, braucht man theoretische Ideen und Methoden, aber die Berechnungen kann man nur mit einem ganz großen und schnellen Rechner durchführen. Für einige Zeit kommt man mit dem Laptop aus, aber für die Lösung von noch komplizierteren Gleichungen reicht er nicht mehr aus.

Auf diese Art und Weise kommt man zum Höchstleistungsrechner. Stellen wir uns vor, dass wir eintausend Laptops haben, die über schnelle Verbindungen verbunden sind. So etwas ist ein Höchstleistungsrechner, der heutzutage mehrere Tausend Prozessoren und eine gewaltige Speicherkapazität hat. Die Rechenleistung wird in Teraflops per Sekunde gemessen. 1 TFlop/s bedeutet 10^12 arithmetische Operationen innerhalb einer Sekunde durchzuführen. Die Speicherkapazität wird in Petabyte gemessen. 1 Pbyte bedeutet 1000 Terabyte=1000*1000 Gigabyte.

Die Höchstleistungsrechner haben in Ungarn insgesamt 448 Tflops/s, 3.2 Pbyte Leistung. Ca. 85% davon befindet sich im Höchstleistungsrechenzentrum der Universität Debrecen. Die weltgrößten Höchstleistungsrechner befinden sich in China, sie haben eine Rechenleistung von 93000 Tflops/s. Sie sind Werkzeuge der modernen Forschung. Wichtig ist dabei, dass diese Rechner nicht in erster Linie von Mathematikern und Informatikern benutzt werden, sondern viel mehr von Physikern, Chemikern, Medizinern, aber auch von Geowissenschaftlern, Juristen und Sprachforschern. Diese Rechner werden auch zur Datenverarbeitung benutzt. Gewaltige Mengen von Messdaten und Beobachtungen werden mit diesen Rechnern verarbeitet, eine Reihe von Aktivitäten, die vorher gar nicht möglich waren.

Deswegen führt das Vorhandensein dieser Rechner unmittelbar zu Forschungsergebnissen. Es ist kein Wunder, dass diese Rechner als grundsätzliche Werkzeuge der modernen Forschung betrachtet werden, und zwar auf jedem Forschungsgebiet.

Um eine andere mögliche Anwendung der Höchstleistungsrechner zu erwähnen, betrachten wir die sogenannten *Mersenne*-Primzahlen. Sie sind der Gestalt, wobei *p* auch eine Primzahl ist. Der Minoritenbruder *M. Mersenne* betrachtete diese Zahlen zuerst, noch im Mittelalter. Es ist immer noch nicht bekannt, ob es unendlich viele *Mersenne*-Primzahlen gibt. Es ist aber gut bekannt, dass es unendlich viele Primzahlen gibt. Es gibt also beliebig große Primzahlen, und es gibt zu jeder Zeit eine größte unter den bekannten Primzahlen. Interessant ist dabei, dass die größte bekannte Primzahl seit sehr langem immer eine *Mersenne*-Primzahl ist. Die ersten *Mersenne*-Primzahlen wurden noch von *Euler* und anderen gefunden. Ende des 20. Jahrhunderts fand u. a. *Slowinski* mehrere *Mersenne*-Primzahlen. In den letzten Jahren wurden alle neuen *Mersenne*-Primzahlen von *GIMPS* gefunden. Es ist keine Person, sondern eine Gesellschaft (*Great Internet Mersenne Prime Search*) von interessierten Mathematikern, die an den numerischen Tests teilnehmen, ob eine Primzahl für *p* ist. Diese

Gesellschaft hat eine Rechenkapazität von insgesamt ca. 250.000 Tflops/s, mehr als der zurzeit größte Höchstleistungsrechner. Es ist ja auch eine Frage von Rechenkapazität, nachdem die Algorithmen zum Primzahltesten entwickelt sind.

In den heutigen Tagen werden noch größere und schnellere Höchstleistungsrechner geplant und gebaut, die in den Forschungen uns allen ganz bestimmt weiterhelfen werden. Wir müssen uns daran gewöhnen, dass diese Geräte normale Werkzeuge der modernen Forschung sind.

Prof. Dr. István GAÁL studierte Mathematik in Debrecen, an der ehemaligen Kossuth Lajos Universität zwischen 1979 und 1984. Seit 1987 arbeitet er am Institut für Mathematik an der Universität Debrecen. 2003 gewann er den akademischen Doktortitel (DSc), und seit 2004 ist er Universitätsprofessor. Von 2005 bis 2016 war er Leiter des Lehrstuhls für Algebra und Zahlentheorie. Als Humboldt-Forschungsstipendiat verbrachte er anderthalb Jahre am Institut für Mathematik der Heinrich-Heine-Universität in Düsseldorf bei Prof. Dr. *M. Pohst*. Er besitzt die folgenden Forschungspreise: Kató Rényi Gedänkpreis, Géza Grünwald Gedänkpreis, Akademiepreis. Zwischen 2010 und 2013 beziehungsweise zwischen 2014 und 2016 war er Vizerektor der Universität Debrecen. Er ist Redakteur der ungarischen Einheit der Zeitschrift Zentralblatt für Mathematik, ferner Redakteur der Zeitungen Publicationes Mathematicae, JP Journal of Algebra and Number Theory, Acta Mat. Acad. Paed. Aegriensis.