Dipl.-Ing. Dr.techn. Clemens Josef Fuchs
Institut für Mathematik A (Analysis und Computational Number Theory)
E-Mail: clemens.fuchs@TUGraz.at
Tel: 0316 873 7127

Diophantische Probleme: Zahlenspielereien und Kryptografie

Diophantine Problems: Number-baubles and Cryptography

Am Beginn jeder Mathematik-Ausbildung steht das Verständnis der verschiedenen Zahlensysteme. Ausgangspunkt sind dabei stets die natürlichen Zahlen von denen schon L. Kronecker gesagt hat „Die natürlichen Zahlen hat der liebe Gott geschaffen, alles andere in der Mathematik ist Menschenwerk". So darf es einen nicht wundern, dass die natürlichen Zahlen bis heute ein reges Forschungsfeld bieten. In meiner Forschung geht es zu einem großen Teil um das Lösen von Diophantischen Problemen, benannt nach Diophantus von Alexandria: dabei werden Lösungen in den natürlichen Zahlen und nicht etwa in den reellen Zahlen für die betrachteten Probleme gesucht. Es werden verschiedenste Methoden, die wiederum aus allen Bereichen der Mathematik kommen, dazu eingesetzt.

Diophantische Gleichungen: Seit Y. Matijasevic im Jahr 1970 bewiesen hat, dass es keinen universellen Algorithmus für die Lösbarkeit einer gegebenen polynomiellen Diophantischen Gleichung gibt, sind Mathematiker auf der Suche nach möglichst großen Klassen von Diophantischen Problemen für die wir die algorithmische Lösbarkeit beweisen können. Es sind aber auch schwächere Aussagen von Interesse, wie z. B. die Herleitung einer oberen Schranke für die Anzahl der Lösungen. Eine interessante Klasse von Diophantischen Gleichungen, die seit kurzem intensiv untersucht wird, sind so genannte exponentiell-polynomielle Gleichungen, wie z. B. $2^n+3^n=x^2$ wobei natürlichen Zahlen n und x als Lösungen gesucht werden. Für solche und allgemeinere Gleichungen konnte ich - teilweise zusammen mit Kollegen von der TU Graz, sowie aus dem Ausland (Italien, Ungarn) - explizite obere Schranken für die Anzahl der Lösungen angeben. Darüber hinaus gilt ein Strukturresultat: eine solche Gleichung kann nur dann unendlich viele Lösungen besitzen, wenn das „offensichtlich" ist (z. B. $18^n+2\cdot6^n+2^n=(18^n+2^n)^2=x^2$).

Diophantische Tupel: Eine Menge von m verschiedenen natürlichen Zahlen, wie z. B. {1,3,8,120}, wird ein Diophantisches m-Tupel genannt, wenn das Produkt von je zwei Zahlen plus ±1 ein Quadrat einer natürlichen Zahl ist. Im obigen Beispiel gilt $1\cdot3+1=2^2$, $1\cdot8+1=3^2$, $1\cdot120+1=11^2$, $3\cdot8+1=5^2$, $3\cdot120+1=19^2$ und schließlich $8\cdot120+1=31^2$; somit handelt es sich um ein Diophantisches Quadrupel. In den letzten Jahren wurden zahlreiche Beiträge zu diesem Thema verfasst, die wichtigsten durch A. Dujella (siehe http:// www.math.hr/dtupels.html). Zum Beispiel konnte er die so genannte Quintupel-Vermutung, die besagt, dass es kein Diophantisches Quintupel mit +1 gibt, nahezu vollständig beweisen. Kürzlich habe ich gemeinsam mit ihm gezeigt, dass es kein Quintupel mit -1 gibt. Damit haben wir gleichzeitig ein altes Problem gelöst, dass auf Diophant und L. Euler zurückgeht: es gibt keine Menge bestehend aus vier positiven natürlichen Zahlen mit der Eigenschaft, dass das Produkt von je zwei solchen Zahlen plus deren Summe das Quadrat einer natürlichen Zahl ist (wie z. B. bei {4,9,28}, denn $4\cdot9+4+9=7^2$, $4\cdot28+4+28=12^2$, $9\cdot28+9+28=17^2$).

Kryptografie: Nachdem die bisher erwähnten Resultate zwar für einen Mathematiker, wohl aber nicht für einen „Anwender" interessant sind, muss erwähnt werden, dass Diophantische Probleme eine wichtige Anwendung in der Kryptografie, also bei der Geheimhaltung von Daten (man denke z. B. an Internetbanking, Emails, E-Commerce oder unser TUGOnline) gefunden haben. Gewisse polynomielle Diophantische Gleichungen haben nämlich eine geometrische Interpretation als sogenannte „elliptische" Kurven. Auf diesen Kurven können Punkte addiert werden. Diese Operation ist leicht ausführbar und wird daher zum Verschlüsseln einer Nachricht verwendet, die Entschlüsselung (d. h. die Bildung der inversen Operation) kann aber nur mit Zusatzinformationen, die wiederum nur Berechtigte haben, effizient ausgeführt werden, womit die Sicherheit gewährleistet werden kann.

Mein Werdegang: Nach dem Studium der Technischen Mathematik an der TU Wien bin ich im Jahr 2000 an die TU Graz gewechselt, wo ich im Rahmen des FWF-Projektes „Algorithmic Diophantine Problems" unter der Leitung von R. Tichy an meiner Dissertation gearbeitet habe, die ich 2002 abschließen konnte. Seitdem bin ich am Institut für Mathematik A als Assistent tätig. Vor kurzem wurde meine Arbeit mit einem Erwin-Schrödinger-Auslandsstipendium des FWF ausgezeichnet. Für weitere Informationen zu meiner Forschung siehe: http://finanz.math.tu-graz.ac.at/~fuchs.

Diophantine Problems: Number-baubles and Cryptography

In my scientific work I am mainly concerned with Diophantine problems: here we are looking for solutions to the problem in the set of integers. To obtain such results methods from all areas of mathematics are utilized.

One of my working areas are Diophantine equations. Here, I obtained - partly in joint work with colleagues from the TU Graz, but also from abroad - explicit upper bounds for the number of solutions of certain families of exponential-polynomial Diophantine equations. Another interesting problem I am dealing with are Diophantine tuples: a Diophantine m-tuple with the property D(n) is a set of different integers with the property that the product of any two of them plus n is a square of an integers. Jointly with A. Dujella I was able to show that there does not exist a D(-n)-quintuple. This result implies an old problem due to Diophant and Euler: there is no set consisting of four positive integers having the property that the product of any two of them plus their sum is a square of an integer. Diophantine problems are used in cryptography, where the aim is to encrypt data in order to protect it from unauthorized usage.

My Vita: I received my MSc in mathematics from the TU Wien and my PhD from TU Graz. Since 2002 I am assistant at the Department of Mathematics A.