Johann Wiesenbauer
TU Wien

Elliptische Kurven in Theorie und Anwendung

Elliptische Kurven nehmen als algebraische Kurven 3.Grades eine in vieler Hinsicht reizvolle Zwischenstellung zwischen den in der Schule vieluntersuchten Geraden und Kegelschnitten einerseits und algebraischen Kurven höherer Ordnung andererseits ein. Außer bei der Auflösung Diophantischer Gleichungen - berühmtestes Beispiel dafür ist wohl der 1995 publizierte Beweis der "Großen Fermatschen Vermutung" - spielen sie auch bei vielen anderen inner- und außermathematischen Anwendungen eine große Rolle.

In dem Vortrag wird u.a. konkret auf ihre Rolle bei deterministischen Primzahltests (ECPP) und bei der Faktorisierung großer Zahlen (ECM), sowie ihre Verwendung bei asymmetrischen Chiffrierverfahren (ElGamal Verfahren etc.) eingegangen, wobei besonderes Augenmerk der algorithmischen Umsetzung mit Hilfe des an Österreichs Mittelschulen weitverbreiteten CAS Derive 5 gilt.