

Algorithmen auf Elliptischen Kurven und ihre Implementierung in DERIVE

Dr. Johann Wiesenbauer

Technische Universität Wien

Die Theorie der Elliptischen Kurven hat bekanntlich in den letzten 10-20 Jahren im Zuge vieler schöner Anwendungen enorm an Bedeutung gewonnen. Außer bei der Auflösung gewisser Diophantischer Gleichungen (berühmtestes Beispiel ist hier wohl der Beweis der Fermatschen Vermutung!), spielen sie auch eine große Rolle bei deterministischen Primzahltests und der Faktorsierung ganzer Zahlen, sowie bei gewissen asymmetrischen Chiffrierverfahren in der Kryptographie. In dem Vortrag werden einige mit Hilfe von DERIVE 5 implementierte Algorithmen vorgestellt, die in diesem Zusammenhang von Bedeutung sind.