Thorsten Kleinjung, Universität Bonn

Primzahlen und Verschlüsselung

Ein altes Problem der Mathematik, große Zahlen schnell in Primfaktoren zu zerlegen, hat in den letzten Jahrzehnten immer größere Bedeutung gewonnen. Ein Verschlüsselungsverfahren, das RSA-Verfahren, beruht nämlich auf diesem Problem, und ein schneller Faktorisierungsalgorithmus würde dieses Verschlüsselungsverfahren unsicher machen. Nach einem Überblick über das Faktorisierungsproblem und das RSA-Verfahren wird ein Faktorisierungsalgorithmus vorgestellt, und es wird über den aktuellen Stand auf diesem Gebiet berichtet.