Philipps Universität Marburg

Fachbereich Mathematik und Informatik

Propädeutikum Mathematik 2020

Große Primzahlen

Referent: Dr. Andreas Lochmann

Zielgruppe: Das Propädeutikum Mathematik ist ein Angebot für Schülerinnen und Schüler der Stufen Q1 bis Q3 an den Schulen in und um Marburg. Die Teilnehmerinnen und Teilnehmer erarbeiten dabei zunächst eigenständig mit Hilfe geeigneter Quellen ein bestimmtes Thema und besuchen anschließend in Kleingruppen einen speziell für sie entwickelten Mathematik-Kurs, der von Hochschullehrerinnen und Hochschullehrern der Philipps-Universität in Zusammenarbeit mit Lehrerinnen und Lehrern der beteiligten Schulen durchgeführt wird.

Anmeldungen für den diesjährigen Kurs werden bis zum 30. September 2020 von den jeweiligen Ansprechpartnern an den Schulen und dem betreuenden Lehrer aller Schulen entgegengenommen:

Herr Günther Kreis
Gymnasium Elisabethschule
Leopold-Lucas-Straße 5
35037 Marburg

Ort und Zeit der Präsenzveranstaltung: Ein oder zwei der Termine 29.10., 5.11., 12.11., 19.11., 26.11., 3.12., jeweils 18:15 - 20:00 Uhr, im Hörsaalgebäude, Biegenstraße 14; voraussichtlich HS +2/0090. Zusätzlich wird eigenständige Mitarbeit erwartet.

Lange Zeit galt die Beschäftigung mit Primzahlen und ihren Eigenschaften als rein intellektuelle Herausforderung, als Beschäftigung zum Training des menschlichen Geistes, aber ohne Anwendung in der realen Welt. Diese Einschätzung hat sich 1976/77 durch die Arbeiten von Diffie, Hellman, Rivest, Shamir und Adleman grundlegend gewandelt. Für moderne Verschlüsselungsverfahren benötigt man große Primzahlen und auch Wissen über Primzahlen und andere Eigenschaften anderer Zahlen. Beispielsweise kann auf einem normalen Laptop binnen einer Sekunde eine Liste der ersten 7 Primzahlen erzeugt werden, die größer als 2,02 Trillionen sind:

2.020.000.000.000.013
2.020.000.000.000.043
2.020.000.000.000.067
2.020.000.000.000.111
2.020.000.000.000.133
2.020.000.000.000.139
2.020.000.000.000.181

Dies ist nicht allein der Geschwindigkeit moderner Computer zu verdanken, sondern auch Verbesserungen in den Berechnungsverfahren zur Bestimmung von Primzahlen. Wir wollen diesen Herbst einige der Ideen, Sätze und Verfahren dahinter kennenlernen.

Geplante Themen:

- Eine kurze Geschichte der Primzahlen
- Modulo-Rechnung und der Satz von Wilson
- RSA-Verschlüsselung
- Das quadratische Reziprozitätstheorem
- Primzahltests

https://www.mathematik.uni-marburg.de/~lochmann/prop2020.html

Kontakt: lochmann@mathematik.uni-marburg.de