Bericht zur Maturarbeit

Ein probabilistischer Primzahltest

Balz Bürgisser, Realgymnasium Rämibühl Zürich

Problemstellung
Primzahlen faszinieren die Menschen seit über 2000 Jahren: Primzahlen treten unregelmässig auf, und sie lassen sich durch keine Formel genau erfassen. Bis heute ist es den Mathematikern nicht gelungen, eine Methode zu entdecken, mit der man bei einer grossen (ungeraden) natürlichen Zahl innert nützlicher Frist feststellen kann, ob sie eine Primzahl ist. In der Not entwickelten die Mathematiker probabilistische Primzahltest: Diese erlauben in kurzer Zeit die Feststellung, dass die vorgegebene natürliche Zahl keine Primzahl ist oder mit einer gewissen Wahrscheinlichkeit eine Primzahl ist; wobei die Wahrscheinlichkeit umso höher wird (und sich 1 nähert), je mehr man den Primzahltest – mit wechselnden Werten für den Parameter – durchläuft.
Der Test von Solovay-Strassen ist ein solcher probabilistischer Primzahltest. Er basiert auf dem Euler-Kriterium: für eine beliebige ungerade Primzahl p gilt $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$ für alle natürlichen Zahlen a mit $1 \le a < p$, wobei $\left(\frac{a}{p}\right)$ das Legendre-Symbol (bzw. das Jacobi-Symbol) bezeichnet. Wenn p eine zusammengesetzte Zahl ist, erfüllen höchstens $\frac{p-1}{2}$ der Zahlen a mit $1 \le a < p$ die obige Kongruenz. Diese Tatsache ergibt einen effizienten Primzahltest.
Der Schüler A interessierte sich für Primzahlen und wollte mit seiner Maturarbeit genauer erkunden, ob er für ein Mathematik-Studium geeignet sei. Ich schlug ihm die Beschäftigung mit dem probabilistischen Primzahltest von Solovay-Strassen vor, was er motiviert in Angriff nahm.

Ergebnisse und Erfahrungen
Der Schüler hat sich zuerst in die Gruppen-, Ring- und Körpertheorie eingearbeitet und sich mit den Restklassenringen Z/mZ beschäftigt. In dieser Phase waren Leitplanken und Ermutigungen notwendig. Das genaue Beweisen eines Sachverhalts wurde an einfachen Sätzen aus der Gruppentheorie eingeübt, beispielsweise am Theorem, dass die Ordnung einer Untergruppe stets die Ordnung der Gruppe teilt.
Dann beschäftigte sich der Schüler mit der Euler Funktion φ. Diese ist ja für eine beliebige natürliche Zahl m definiert als φ(m) = Anzahl zu m teilerfremde natürliche Zahlen < m . Dann „entdeckte“ er den Satz von Euler-Fermat: Für eine beliebige natürliche Zahl m gilt $a^{\varphi(m)} \equiv 1 \bmod m$ für alle zu m teilerfremden a. Ein wichtiges Erlebnis für den Schüler war, als er erkannte, dass der Beweis dieses Satzes elegant und einfach wurde, wenn man die Gruppentheorie auf die multiplikative Gruppe der teilerfremden Restklassen (Z/mZ)* anwendet.
Dann war der Maturand nicht mehr zu halten: Er beschäftigte sich mit dem Legendre- und dem Jacobi-Symbol und bewies das Euler-Kriterium mit eigenen Überlegungen detailliert.
Von da war es nur noch ein kleiner Schritt zur Formulierung des Theorems von Solovay-Strassen; dessen genauer Beweis war allerdings ein harter Brocken, da der chinesische Restsatz mehrmals geschickt angewendet werden muss. Der Maturand hat eigene Ideen und Wege in den Beweis eingebracht und sich so intensiv mit ihm auseinandergesetzt, dass er sogar eine Verschärfung des Theorems entdeckte. Aus dem Theorem leitete er den Primzahltest von So-

lovay-Strassen ab: Er beschrieb den Algorithmus in einem Flussdiagramm und berechnete die Anzahl Iterationen, um mit 99-prozentiger Sicherheit eine ungerade natürliche Zahl als Primzahl zu identifizieren. Beispielsweise berechnete der Schüler selbständig, dass eine hundertstellige ungerade Zahl mittels dem Test von Solovay-Strassen in 15 Durchläufen mit mindestens 99-prozentiger Sicherheit als Primzahl (und mit 100-prozentiger Sicherheit als zusammengesetzte Zahl) erkannt werden kann.

Bemerkungen
Der Schüler A belegte das neusprachliche Maturitätsprofil. Er war seit einigen Jahren durch sein Interesse und seine Begabung im mathematisch-naturwissenschaftlichen Bereich aufgefallen. Er kam zu mir, da er die Maturarbeit in Mathematik schreiben wollte – und zwar wolle er sich mit Primzahlen beschäftigen und zugleich sein Studium an der ETH genau bestimmen und vorbereiten. Probabilistische Primzahltests haben ihn sofort fasziniert und intrinsisch so stark motiviert, dass er sich selbständig in höhere Algebra und Zahlentheorie einarbeitete. Das schrittweise logische Schliessen beim Beweisen und auch das präzise Formulieren eines mathematischen Sachverhaltes haben wir zusammen in mehreren Besprechungen geübt.

Literatur:
Neben zahlreichen Quellen im Internet benützte A. folgende Bücher:

- Amann, Herbert und Escher, Joachim. Analysis 1, dritte Auflage, Birkhäuser Verlag: Basel-Boston-Berlin 2007. ISBN 3-7643-7755-0
- Lugowski, Herbert und Weinert, Hann Joachim. Grundzüge der Algebra, vierte Auflage, Verlag B.G. Teubner: Leipzig 1957
- Remmert, Reinhold und Ullrich, Peter. Elementare Zahlentheorie, dritte Auflage, Birkhäuser-Verlag: Basel-Boston-Berlin 2008. ISBN 978-3-7643-7730-4
- Scheid, Harald und Frommer, Andreas. Zahlentheorie, vierte Auflage, Spektrum Akademischer Verlag: München 2007. ISBN 978-3-8274-1692-6