Katharina KLEMBALSKI, Berlin

# Primzahltests als innermathematische Vernetzung von Zahlentheorie und Wahrscheinlichkeitsrechnung

Große Primzahlen sind ein wesentlicher Konstruktionsbestandteil weit verbreiteter kryptografischer Algorithmen. Auch wenn das Wissen über die Erzeugung von Primzahlen (ebenso wie die kryptografischen Verfahren) aus Anwendersicht *nicht* notwendig ist, so ist es mit Schülern gut zu thematisieren. Primzahltests sind somit geeignet, um (exemplarisch) die *verborgene* und gleichzeitig moderne Mathematik unseres durch Technik und mithin mathematisch geprägten Alltags sichtbar zu machen. Überraschenderweise sind es Methoden der Stochastik, die das innerhalb der Zahlentheorie grundsätzlich exakt lösbare Problem, solche Zahlen zu finden, in der Praxis zugänglich machen. Günstig für den Unterricht ist es, dass dafür nur wenig zusätzliches Wissen bereitgestellt werden muss.
Besondere Chancen für den Mathematikunterricht bestehen darin, dass Schüler

- sich mit einem authentischen Problem der modernen Mathematik beschäftigen.
- zwei mathematische Herangehensweisen zur Lösung eines Problems verbinden: die zufallsbestimmte der Stochastik und das (scheinbar) exakte Vorgehen aus der restlichen Schulmathematik. Der Beitrag der Stochastik zur Lösung eines innermathematischen Problems steht im besonderen Kontrast zu den dominierenden außermathematischen Bezügen der Stochastik.
- Probabilistik als (durch den Computer zugängliche) Denkweise zum Problemlösen erfahren.

Wesentliche mathematische Grundlagen einer entsprechenden Unterrichtseinheit sind das Rechnen mit Kongruenzen, der kleine Satz von Fermat (Wahlpflichtunterricht Kl. 9/10) sowie mehrstufige Zufallsexperimente (Kl. 9/10) [1]. Nahe liegende Orte der Integration in den Schulunterricht sind daher insbesondere im Anschluss an die entsprechenden Elemente der Zahlentheorie oder Stochastik angesiedelt.

Meldungen aus der Presse über neue größte (bekannte) Primzahlen oder Faktorisierungsrekorde [u.a. 6, 7] können Anlass sein, die scheinbar vertrauten Primzahlen vom höheren Standpunkt zu betrachten. Ein anderer Zugang ergibt sich ausgehend von asymmetrischen Kryptosystemen, deren Si-

cherheit auf dem Einsatz großer Primzahlen beruht.[1]

Ein natürliches Vorgehen auf der Suche nach Primzahlen ist es, einen Primzahlkandidaten $p$ durch alle (Prim)Zahlen kleiner der Quadratwurzel von $p$ probehalber zu dividieren. Das nach ähnlichem Prinzip funktionierende Sieb des Eratosthenes liefert eine Liste aller Primzahlen kleiner gleich $p$. Die Suche nach einer möglichst großen Primzahl wird Schüler jedoch schnell zu Grenzen des Taschenrechereinsatzes bzw. der eingesetzten Software führen.
Systematisches Testen der Primzahleigenschaft ausgewählter Zahlen – zunächst per Hand, dann mit einem CAS – illustriert, dass der Berechnungsaufwand mit zunehmender Stellenzahl von $p$ stärker steigt als durch den Einsatz von Computern ausgeglichen werden kann.[2] Hintergrund ist der exponentiell zur Stellenzahl steigende Berechnungsaufwand. Beispielsweise benötigt MATHEMATICA (6.0, 1.5 GHz) für die Bestimmung der Primfaktorzerlegung der 50 bzw. 100stelligen Zahlen $p_1$ und $p_2$ nur 3ms bzw. 8ms. Hingegen wurde der Versuch, die Primalität von $p_3 = p_1 p_2$ durch Faktorisieren zu widerlegen, nach einer Woche abgebrochen.[3]
$p_1 = 94287619113665765837947743093327783016721912346 47$
$p_2 = 47455032265804039922794668036139134834983405258209091831 23050894575258287816036082748631537889230 37$
Der MATHEMATICA-Befehl „PrimeQ[$p$]“ benötigt erheblich weniger Zeit und liefert Aussagen über Primalität ohne Rückgriff auf die Primfaktorzerlegung: 2ms ($p_1$), 10ms ($p_2$) bzw. 14ms ($p_3$). Wie aber können die Zahlen ohne Zerlegung auf Zusammengesetztheit überprüft werden? Hinter dem genannten Befehl verbirgt sich der Miller-Rabin-Test.

Dessen zahlentheoretische Grundlagen sind der *kleine Satz von Fermat* und der von *Miller*. *Fermat*: Für Primzahlen $p$ mit $(a, p) = 1$ gilt

$$a^{p-1} \equiv 1 \bmod p.$$

Die Umkehrung gilt nicht. Beispielsweise ist $2^{341-1} \equiv 1 \bmod 341$, aber $341 = 11 \cdot 30$ ist zusammengesetzt. Zahlen mit dieser Eigenschaft heißen *pseudoprim zur Basis a*. Sogenannte *Carmichaelzahlen* sind sogar zu allen Basen pseudoprim. Es gibt sogar unendlich viele Carmichaelzahlen. Wie

1 RSA oder auch der Diffie-Hellman-Schlüsseltausch arbeiten mit Hilfe von Primzahlen mit mehr als 150 Stellen [1]. Sie sind Sicherheitselemente des verbreiteten SSL-Protokolls, mit dem via Internet ausgetauschte Daten verschlüsselt werden.

2 Das steht durchaus im Widerspruch zur Schulerfahrung, das der Einsatz größerer (Stellen)Zahlen durch den Taschenrechnereinsatz ausgeglichen wird.

3 Der MATHEMATICA-Befehl FactorInteger[n] nutzt für große Zahlen zwar fortgeschrittenere Algorithmen als die einfache Probedivision, aber auch deren Laufzeit ist von exponentieller Laufzeit in Abhängigkeit von $p$.

können wir trotzdem auf die Primalität einer Zahl schließen? Betrachten wir zunächst einige Folgerungen aus dem kleinen Satz von Fermat. Für Primzahlen $p > 2$ gilt: $a^{p-1} \equiv 1 \bmod p \Leftrightarrow a^{p-1} - 1 \equiv 0 \bmod p$
$\Leftrightarrow a^{(p-1)/2} - 1)( a^{(p-1)/2} + 1) \equiv 0 \bmod p$, da $p - 1$ gerade ist.
$\Leftrightarrow (a^{(p-1)/4} - 1)(a^{(p-1)/4} + 1)(a^{(p-1)/2} + 1) \equiv 0 \bmod p$, falls 2 auch $(p - 1)/2$ teilt. Ebenso folgt für $d = (p - 1)/2^k$ mit $k$ als höchste 2er-Potenz, die $p - 1$ teilt:
$\Leftrightarrow (a^d - 1)(a^d + 1) \ldots (a^{(p-1)/2} + 1) \equiv 0 \bmod p$.
Da $p$ prim ist, muss einer der Faktoren kongruent Null und somit $a^d$ kongruent $\pm 1$ sein; oder eine der folgenden Potenzen ist kongruent $-1 \pmod p$.
Um nun einen Kandidaten $p$ auf Primalität zu testen, berechnen wir für eine zu $p$ teilerfremde Basis $a < p$ die Potenzen $a^d, \ldots a^{(p-1)/4}, a^{(p-1)/2} \pmod p$.
Der Test auf Primalität gilt als erfolgreich, wenn $a^d \equiv \pm 1 \bmod p$ oder eine der folgenden Potenzen kongruent $-1$ ist. Im anderen Fall ist $p$ eindeutig als zusammengesetzt identifiziert. Besteht $p$ den Test, so heißt *a Zeuge* gegen die Zusammengesetztheit von $p$.
Welche Aussagekraft hat dieser Test? Wegen des Satzes von Fermat kann keine Primzahl fälschlich als zusammengesetzt identifiziert werden. Umgekehrt ist es möglich, dass eine zusammengesetzte Zahl, für die gewählte Basis den Test besteht. Eine solche Zahl heißt *starke Pseudoprimzahl zur Basis a*. Beispielsweise gilt für $p = 781$: $5^{781-1} \equiv ((5^{195})^2)^2 \bmod 781$ und $5^{195} \equiv 1 \bmod 781$, d.h. 5 ist Zeuge gegen die Zusammengesetzheit von 781, aber es ist $781 = 11 \cdot 71$.
Glücklicherweise lässt sich die Zahl solcher Basen nach oben abschätzen [1, S. 129]: Maximal für ein Viertel aller möglichen Basen $a$ besteht eine zusammengesetzte Zahl $p$ fälschlicherweise diesen Test (Satz von Miller).
Die zentrale Idee des Miller Rabin-Tests ist es, diese zahlentheoretisch gewonnene Abschätzung mit einem probabilistischen Verfahren zu kombinieren. Denn besteht eine Zahl mit einer (zufällig gewählten) Basis den Test, so lässt sich durch Wiederholung mit anderen Basen die Fehlerwahrscheinlichkeit mit jedem Durchlauf um den Faktor 4 verringern. Nach $r$ Wiederholungen beträgt die Fehlerwahrscheinlichkeit daher höchstens $(¼)^r$. Die Sicherheit des Tests kann also durch die Wahl von $r$ beliebig erhöht werden.

Anknüpfungspunkte und Vertiefungen im Unterricht ergeben sich je nach dem Vorwissen der Schüler und dem Umfang einer entsprechenden Unterrichtseinheit. Zu reflektieren ist in jedem Fall die Algorithmisierbarkeit der einzelnen Rechenschritte und deren Ausführung durch den Computer, die erst die fruchtbare Kombination von Zahlentheorie und Stochastik möglich macht. Vertiefungen sind insbesondere durch den euklidischen Algorithmus bzw. den des schnellen Potenzierens möglich. Andere Vertiefungen in

Richtung Zahlentheorie sind gegeben durch die Beweise des Satzes von Fermat und des Satzes von Miller (bzw. einer leichter beweisbaren Abschätzung durch ½ statt ¼ [vgl. 5]), wobei letzterer in Relation zum Primzahltest elementar sehr aufwändig ist.
Fragen, die vorhandenes Wissen der Stochastik einbinden sind die Folgenden: Wie finde ich eine zufällige Basis *a*? Und ähnlich: Wie finde ich einen zufälligen Kandidaten *p*? Wieso ist die Abschätzung von ¼ auch bei mehrfacher Durchführung korrekt? Was heißt *beliebig sicher*?
Die letzte Frage ist nicht trivial, denn es scheint überraschend, wenn nicht sogar „unmathematisch", in sicherheitskritischen Anwendungen nur „primzahlverdächtige" Zahlen zu verwenden. Das durch Wahl von *r* beliebig hohe Maß an Sicherheit ist daher als spezifische Anforderung an ein probabilistisches Verfahren hervorzuheben. Für ausgewählte Werte von *r* sollte dieses von Schülern durch Vergleich mit geeigneten Ereignissen fassbar gemacht werden.

Zum Abschluss wollen wir hervorheben, dass es sich bei dem vorgestellten probabilistischen Nachweis der Primzahleigenschaft nicht um einen Beweis im engen mathematischen Sinn handelt, denn absolute Sicherheit gibt es hier nicht.[4] Jedoch gewinnt man durch diesen Verzicht ein Werkzeug für Probleme jenseits der klassischen Beweis- und Berechenbarkeit, die sonst nur schwer oder gar nicht zugänglich sind.
Stichworte für weitere Anwendungen, die sich ähnliche Prinzipien zunutze machen seien Zero-Knowledge-Protokolle [2] und Monte-Carlo-Algorithmen zur Berechnung von Integralen [4].

## Literatur


[1] Senatsverwaltung für Bildung, Jugend und Sport Berlin (2006): Rahmenlehrplan für die Sekundarstufe I Mathematik.
[2] Beutelspacher, A.; Schwenk, J.; Wolfenstetter, K.-D. (2006): Moderne Verfahren der Kryptografie von RSA zu Zero-Knowledge. Vieweg.
[3] Buchmann, J. (2005): Einführung in die Kryptologie. Springer.
[4] Shonkwiler, R. W.; Mendivil, F. (2009): Explorations in Monte Carlo methods. Springer.
[5] Lasse, R.; Waldecker, R. (2009): Primzahltests für Einsteiger. Vieweg+Teubner.
[6] Unbekannt: Neuer Entschlüsselungsrekord: Einen sogenannten RSA-Schlüssel von 768 Bit. Spiegel Online, Meldung vom 8.1.2010.
[7] Dambeck, H.: Zwei neue Rekordprimzahlen entdeckt. Spiegel Online, Meldung vom 13.9.2008.


4 Es sei denn, der Test wird mit hinreichend vielen Basen wiederholt. Jedoch würde wegen des resultierenden Aufwandes für große Kandidaten *p* der Einsatz des Primzahltests hinfällig.