Was können Schüler anhand von Primzahltests über Mathematik lernen?

Innermathematisches Vernetzen von Zahlentheorie und Wahrscheinlichkeitsrechnung

Katharina Klembalski

Humboldt-Universität Berlin

20. April 11

Rekordwurm aus 9,8 Millionen Ziffern

9.808.358 Ziffern, Punkt nicht mitgezählt: Das ist die neueste größte Primzahl. Zwei US-amerikanische Mathematiker haben "M32582657" entdeckt - mit Hilfe von 700 Computern, die neun Monate lang gerechnet haben.

Zwei neue Rekord-Primzahlen entdeckt

Von Holger Dambeck

Sie haben mehr als zehn Millionen Stellen: Mit Computerhilfe wurden zwei weitere Primzahlen entdeckt - ein neuer Rekord. Bei der Jagd nach immer größeren unteilbaren Ziffern geht es um sichere Datenverschlüsselung. Und um 100.000 Dollar.

Forscher stellen Entschlüsselungsrekord auf

Neuer Entschlüsselungsrekord: Einen sogenannten RSA-Schlüssel von 768 Bit Länge knackte ein Forscherteam mit Hilfe eines Rechnernetzwerks - und jahrelanger Arbeit. In zehn Jahren, fürchten die Wissenschaftler, könnte die nächste Hürde fallen - und die schützt auch Kreditkartendaten.

Warum Primzahltests im Mathematikunterricht?

- angewandte Mathematik
  - alltägliche Relevanz für jeden Einzelnen
  - verborgene Mathematik sichtbar machen
  - wenig zusätzliches Wissen erforderlich
- Mathematik heute
  - Gegenstand der Forschung – Brücke Schule - Hochschule
  - Diskrete Mathematik
  - Computer als Mittel und Anlass mathematischer Forschung

Besondere Chance für den Mathematikunterricht

- Schüler beschäftigen sich mit einem authentischen Problem der modernen Mathematik (1980)
- Schüler verbinden Wissen (bis dahin) unabhängiger, mathematischer Teildisziplinen zur Lösung des Problems
- Schüler erfahren Stochastik als (durch den Computer zugängliche) Denkweise zum Problemlösen.

Bereit zu stellendes Hintergrundwissen

- Zahlentheorie
  - Rechnen mit Kongruenzen
  - Kleiner Satz von Fermat (17. Jh.)
  - Satz von Rabin (1980)
- Wahrscheinlichkeitsrechnung
  - Mehrstufige Zufallsexperimente, Pfadregeln
  - Simulationen (20. Jh.)

Möglicher Zeitpunkt des Unterrichtens

- Zahlentheorie & Kryptografie
  - Wahlpflichtunterricht Mathematik (Klasse 9/10)
  - Informatik SEK II
- Wahrscheinlichkeitsrechnung
  - Mathematik Klasse 10
- als Projekt in Vertiefungs-, Seminarkursen (SEK II)

Eine mögliche Einbettung in den Unterricht

Wie finde ich große Primzahlen?

- Wieviele Primzahlen gibt es in einem bestimmten Intervall?
  $(\pi(n) \to \frac{n}{\ln(n)})$
- Wie sind Primzahlen verteilt?
  (Primzahllücken, -zwillinge)
- Wie erkenne ich Primzahlen?

Aufgabe

- Finde alle Primzahlen kleiner 400.
- Finde eine möglichst große Primzahl.

Experimentieren mit Mathematica[1]

- $p = 942876191136657658379477430933277830167219$
  `FactorInteger[p]` in 2,3 s sowie `PrimeQ[p]` in 1/1000 s.
- $p = 213598703592091008239502318434121854383503 4 \cdots$
  $063300427548372221691024699701104537360439015839 \cdots$
  9606479
  `FactorInteger[p]` in s sowie `PrimeQ[p]` in 3/1000 s.

[1] kostenfrei auf www.wolframalpha.com oder mit dem CAS Maxima (OpenSource)

Schülervortrag: Miller-Rabin-Test

Eigenschaften von (Pseudo-)Primzahlen

Kleiner Satz von Fermat
Sei p eine Primzahl und a eine natürliche Zahl mit $(a, p) = 1$.
Dann gilt:

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

Beispiel

- $6^{101-1} \equiv 1 \bmod 101$

Eigenschaften von (Pseudo-)Primzahlen

weitere Beispiele

- $2^{341-1} \equiv 1 \bmod 341$ aber $341 = 11 \cdot 31$

  $\Rightarrow$ 341 heißt *Pseudoprimzahl zur Basis* 2.
- $3^{341-1} \equiv 56 \bmod 341$

  $\Rightarrow$ 341 ist *keine* Pseudoprimzahl zur Basis 3
- $2^{561-1} \equiv 1 \bmod 561$ und $561 = 3 \cdot 11 \cdot 17$

  leider gilt auch $5^{561-1} \equiv 1 \bmod 561$ sowie

  $a^{561-1} \equiv 1 \bmod 561$ für alle $(a, 561) = 1$.

  Es gibt unendlich viele Carmichaelzahlen.

Aus dem Satz von Fermat folgt ...

Es sei $p > 2$ prim und $(a, p) = 1$, dann gilt:

$$
\begin{aligned}
a^{p-1} &\equiv 1 \bmod p &&\iff \\
a^{p-1} - 1 &\equiv 0 \bmod p &&\iff \\
(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) &\equiv 0 \bmod p &&\iff \\
(a^{\frac{p-1}{4}} - 1)(a^{\frac{p-1}{4}} + 1)(a^{\frac{p-1}{2}} + 1) &\equiv 0 \bmod p &&\iff \\
&\dots \\
(a^{\frac{p-1}{2^k}} - 1)(a^{\frac{p-1}{2^k}} + 1)(a^{\frac{p-1}{2^{k-1}}} + 1) \dots (a^{\frac{p-1}{2}} + 1) &\equiv 0 \bmod p
\end{aligned}
$$

k sei die höchste Potenz die $p - 1$ teilt.

Aus dem Satz von Fermat folgt ...

$$(a^{\frac{p-1}{2^k}} - 1)(a^{\frac{p-1}{2^k}} + 1)(a^{\frac{p-1}{2^{k-1}}} + 1) \dots (a^{\frac{p-1}{2}} + 1) \equiv 0 \bmod p$$

Da p eine Primzahl ist, muss gelten

$$a^{\frac{p-1}{2^k}} \equiv 1 \bmod p \text{ oder}$$

$$a^{\frac{p-1}{2^k}} \equiv -1 \bmod p \text{ oder}$$

$$a^{\frac{p-1}{2^{k-1}}} \equiv -1 \bmod p \text{ oder}$$

$$\dots$$

$$a^{\frac{p-1}{2}} \equiv -1 \bmod p$$

Test auf Primalität von p

Berechnen der Folge $a^{\frac{p-1}{2^k}}, a^{\frac{p-1}{2^{k-1}}} \ldots, a^{p-1} \pmod{p}$

$$a^{p-1} \equiv (((\underbrace{a^{\frac{p-1}{2^k}}}_{\equiv \pm 1})^2 \ldots)^2)^2 \bmod p$$

$$\underbrace{\qquad\qquad\qquad\qquad}_{\text{oder } \equiv -1}$$

$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{\text{oder } \equiv -1}$$

p besteht den Test, wenn die Folge die folgende Gestalt besitzt:

- $(\pm 1, 1, \ldots, 1)$ oder
- $(X, \ldots, X, -1, 1, \ldots, 1)$ und $X \neq \pm 1$

Beispiele – Aufgaben während des Vortrages

- $6^{101-1} \equiv ((\underbrace{6^{25}}_{\equiv -1})^2)^2) \bmod 101$
  $\underbrace{\underbrace{\equiv 1}_{\equiv 1}}_{\equiv 1}$

  $\Longrightarrow$ 101 ist ein Primzahlkandidat.

- $2^{561-1} \equiv (((\underbrace{2^{70}}_{\equiv 166})^2)^2)^2 \bmod 561$
  $\underbrace{\underbrace{\underbrace{\equiv 67}_{\equiv 1}}_{\equiv 1}}_{\equiv 1}$

  $\Longrightarrow$ 561 ist zusammengesetzt; 2 heißt *Zeuge* für die Zusammengesetztheit von 251.

Beispiele – Aufgaben während des Vortrages

$$5^{781-1} \equiv ((\underbrace{5^{195}}_{\equiv 1})^2)^2 \bmod 781$$

$$\underbrace{\quad\quad}_{\equiv 1}$$

$$\underbrace{\quad\quad\quad\quad}_{\equiv 1}$$

aber

$$781 = 11 \cdot 71$$

781 heißt *starke Pseudoprimzahl zur Basis* 5.

Besteht ein Kandidat p den Test?

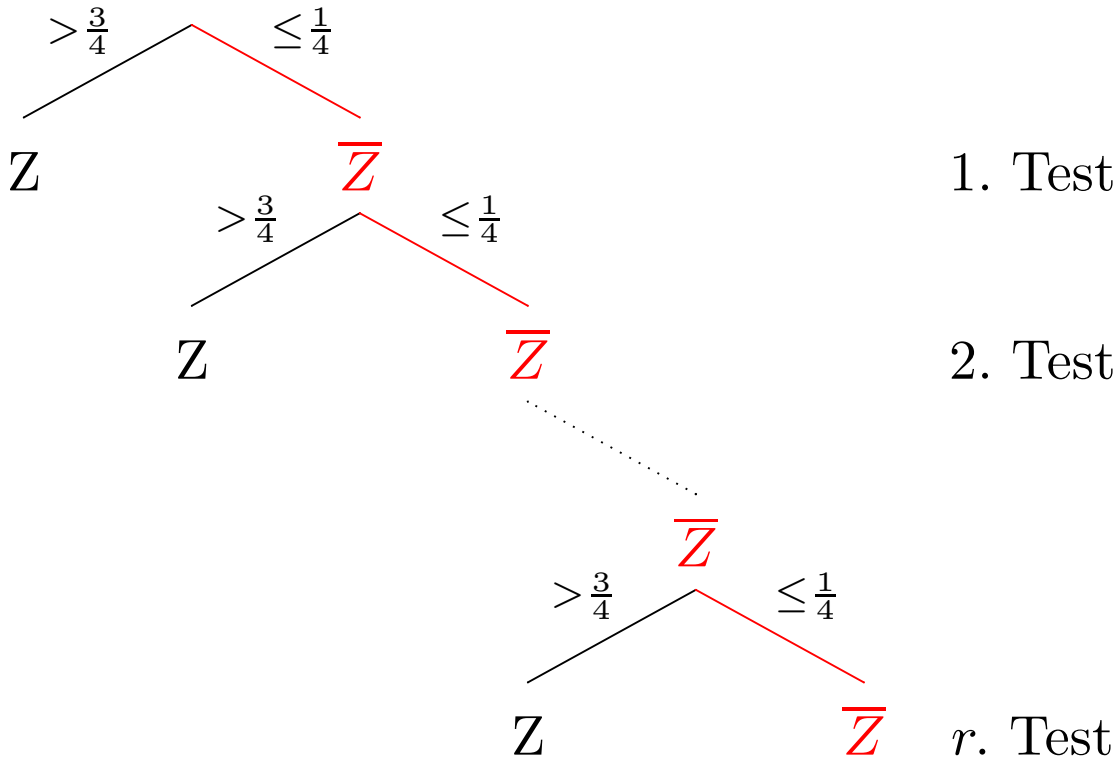
- nein – Dann ist p sicher zusammengesetzt. Wegen des kleinen Fermats ist ausgeschlossen, dass Primzahlen als zusammengesetzt erkannt werden.
- ja – Dann ist p vielleicht eine Primzahl. Die Aussage ist nicht sicher, da zusammengesetzte Zahlen fälschlich als prim identifiziert werden können. Die Fehlerwahrscheinlichkeit kann jedoch nach oben abgeschätzt werden.

Satz von Rabin

Sei p zusammengesetzt. Dann sind höchstens ein Viertel aller Basen kleiner p keine Zeugen für die Zusammengesetztheit von p.

Konstruktion des probabilistischen Tests

Sei p zusammengesetzt und
$Z :=$ *a* sei Zeuge für die Zusammengesetztheit von p.



Es gilt: $P(p \text{ besteht den Test} \mid p \text{ ist zusammengesetzt}) \leq \left(\frac{1}{4}\right)^r$.

Konstruktion des probabilistischen Tests

Sei p ein Kandidat für eine Primzahl.
Für $i = 1, \ldots r$ tue das Folgende:

- Wähle ein zufälliges $a < p$.
- Prüfe, ob $(a, p) = 1$.
- Falls $(a, p) \neq 1$,so antworte: p ist zusammengesetzt.
  Sonst teste auf Primalität:
  Gilt nicht $a^{p-1} \equiv (((\underbrace{a^{\frac{p-1}{2^k}}}_{\equiv \pm 1})^2 \ \ldots)^2)^2 \bmod p$,
  $\underbrace{\underbrace{\text{oder } \equiv -1}}_{\text{oder } \equiv -1}$
  so antworte: p ist zusammengesetzt.

Sonst antworte: p ist (fast sicher) eine Primzahl.

Anknüpfungen Zahlentheorie

- Beweis des Satzes von Fermat
- Prüfe, ob $(a, p) = 1$ (Euklidischer Algorithmus)
- Bestimme $a^{\frac{p-1}{2^k}}, a^{\frac{p-1}{2^{k-1}}} \ldots, a^{p-1} (\mathrm{mod}\, p)$ (Square & Multiply-Algorithmus)
- Abschätzung der falschen Zeugen gegen Zusammengesetztheit

Anknüpfungen Stochastik

- Wähle zufälliges $a < p$ mit . . .
- Was heißt beliebig sicher?
- Abschätzung der falschen Zeugen gegen Zusammengesetztheit
- Simulationen

Aufgabe

Erzeuge eine zufällige 30stellige Zahl, benutze die Funktion `ZUFALLSZAHL()` oder `ZUFALLSBEREICH(min,max)`. Gib eine Vorschrift zur Erzeugung von Zufallszahlen beliebiger Länge an.

Beliebig sicher? – Nur fast sicher nicht zusammengesetzt!

Aufgabe

Welche Größenordnung verbirgt sich hinter $(1/4)^{30} \approx 9 \cdot 10^{-19}$? Veranschauliche den Zahlenwert anhand geeigneter Wahrscheinlichkeiten.

Die Chance auf einen 6er im Lotto (mit Superzahl) zwei Wochen hintereinder ist 100mal größer.

Ist das Mathematik?

Probabilistik vs. Exaktheit

Aufgabe

Überprüfe die oben bestimmten Primzahlen jeweils auch mit dem anderen Verfahren auf Primalität. Welches Verfahren ist besser? Nach welchen Kriterien entscheidest Du?

theoretisch vs. praktisch
exakt vs. unsicher
langsam vs. schnell (effizient)

Vielen Dank