ETH zürich

Primzahltests

Patrick Amrein
Alessandro Lägeler
Markus Schwagenscheidt

Primzahlen

In der Kryptographie benötigt man häufig **große Primzahlen.**

Erinnerung: Eine Primzahl p ist eine Zahl > 1, die nur durch sich selbst und 1 teilbar ist.

Beispiele von Primzahlen

$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23, \ldots,\ 101,\ 103,\ 107,\ 109,\ 113,\ 127, \ldots, 65789, \ldots,\ 2^{82589933} - 1, \ldots.$

Aufgaben:

1. Zeige, dass 487 eine Primzahl ist.
2. Zeige, dass 899 keine Primzahl ist.
3. Zeige, dass jede zusammengesetzte Zahl n einen Primteiler $p \leq \sqrt{n}$ hat.

Primfaktorzerlegung

Satz über die eindeutige Primfaktorzerlegung

Jede natürliche Zahl $n \in \mathbb{N} = \{1, 2, 3, \dots\}$ mit $n > 1$ besitzt eine eindeutige Primfaktorisierung

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

mit Primzahlen $p_1 < p_2 < \cdots < p_k$ und natürlichen Zahlen $e_1, \dots, e_k \in \mathbb{N}$.

Aufgabe: Bestimme die Primfaktorzerlegung von 20454.

Problem: Die Bestimmung der Primfaktorzerlegung großer Zahlen n ist **sehr aufwändig**, wenn n nur große Primfaktoren hat.

Wieviele Primzahlen gibt es?

Satz (Euklid, ca. 200 v.Chr.)

Es gibt unendlich viele Primzahlen.

Beweis. Nehmen wir an, es gäbe nur **endlich viele** verschiedene Primzahlen $p_1, p_2, \ldots, p_k$.

Wir bilden die Zahl

$$m = p_1 \cdots p_k + 1.$$

Es gibt zwei mögliche Fälle:

1. m ist selbst eine Primzahl.
   Das kann aber nicht sein, da m größer als jede der Primzahlen $p_1, \ldots, p_k$ ist.
2. m ist also keine Primzahl. Wegen der Primfaktorzerlegung ist m durch eine der Primzahlen $p_1, \ldots, p_k$ teilbar, sagen wir p_j. Dann wäre aber auch $1 = m - p_1 \cdots p_k$ durch p_j teilbar, was nicht möglich ist.

Insgesamt erhalten wir einen **Widerspruch**.

Daher muss unsere **Annahme**, dass es nur endlich viele Primzahlen gibt, **falsch** sein. □

Primzahlen finden

Das **Sieb des Eratosthenes** ist eine Methode zum Auflisten von Primzahlen.

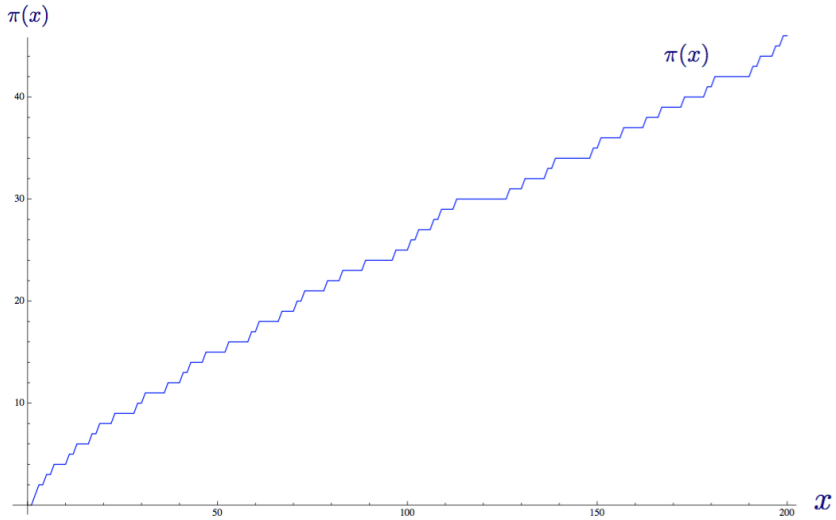
Wie *häufig* sind Primzahlen?

Bertrands Postulat: Für jede natürliche Zahl n gibt es mindestens eine Primzahl zwischen n und $2n$.

Beispiel. Es gibt eine Primzahl zwischen 1000 und 2000.

Aufgabe: Finde Primzahlen zwischen n und $2n$ für jedes $n \leq 100$.

Wie *häufig* sind Primzahlen?



$\pi(x) =$ Anzahl der Primzahlen $\leq x$

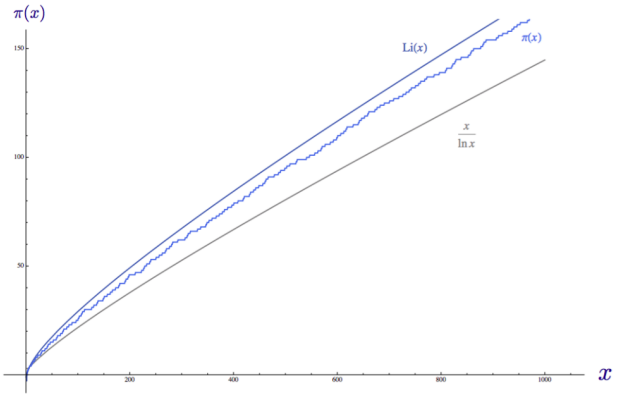
Wie *häufig* sind Primzahlen?

Primzahlsatz (Hadamard, de La Vallée Poussin, 1896).

$\pi(x)$ verhält sich wie $\frac{x}{\ln(x)}$ für große x.

Eine etwas bessere Approximation ist durch $\mathrm{Li}(x) = \int_2^x \frac{dt}{\ln(t)}$ gegeben.

Die **Wahrscheinlichkeit**, dass eine zufällige Zahl in {1,...,n} eine Primzahl ist, ist etwa $\frac{1}{\ln(n)}$.



Erzeugung großer Primzahlen

In der Kryptographie, z.B. beim **RSA-Verfahren**, benötigt man **sehr große Primzahlen**.

Dazu wählt man eine **zufällige Zahl** n und **testet** dann, ob n eine Primzahl ist.

Erzeugung großer Primzahlen

In der Kryptographie, z.B. beim **RSA-Verfahren**, benötigt man **sehr große Primzahlen**.

Dazu wählt man eine **zufällige Zahl** n und **testet** dann, ob n eine Primzahl ist.

In der Praxis benutzt man **probabilistische Primzahltests**.

Das Ergebnis ist entweder

1. "n ist **keine** Primzahl" oder
2. "n ist **wahrscheinlich** eine Primzahl".

Erzeugung großer Primzahlen

In der Kryptographie, z.B. beim **RSA-Verfahren**, benötigt man **sehr große Primzahlen**.

Dazu wählt man eine **zufällige Zahl** n und **testet** dann, ob n eine Primzahl ist.

In der Praxis benutzt man **probabilistische Primzahltests**.

Das Ergebnis ist entweder

1. "n ist **keine** Primzahl" oder
2. "n ist **wahrscheinlich** eine Primzahl".

Durch **mehrfache Wiederholung des Tests** kann die Wahrscheinlichkeit, dass man fälschlicherweise eine zusammengesetzte Zahl für eine Primzahl hält, sehr klein gehalten werden.

Primzahltests

Grundidee der Primzahltests

Finde eine **leicht zu überprüfende** Eigenschaft, die **jede Primzahl** besitzt, die aber nur von **möglichst wenigen zusammengesetzten Zahlen** erfüllt wird.

Beispiel

Nach dem kleinen Satz von Fermat gilt für jede Primzahl p

$$a^{p-1} \equiv 1 \pmod{p}$$

für jede zu p teilerfremde Zahl a.

Folgerung: Gilt

$$a^{n-1} \not\equiv 1 \pmod{n}$$

für ein a, so kann n nicht prim sein!

Aufgabe: Zeige mit obiger Idee, dass $n = 6$ keine Primzahl ist.

Der Fermatsche Primzahltest

Eingabe: Eine natürliche Zahl n.

Ausgabe:

- Falls n **prim**: "n `wahrscheinlich prim`".
- Falls n **nicht prim**: Entweder "n `zusammengesetzt`" oder "n `wahrscheinlich prim`".

Fermatscher Primzahltest

1. Wähle ein zufälliges $a \in \{2, \ldots, n-2\}$.
2. Ist $\mathrm{ggT}(a, n) > 1$, gib "n `zusammengesetzt`" aus.
3. Falls
$$a^{n-1} \equiv 1 \pmod{n},$$
gib "n `wahrscheinlich prim`" aus.
4. Falls die Bedingung nicht erfüllt ist, so ist n zusammengesetzt.
Gib "n `zusammengesetzt`" aus.

Fragen beim Fermatschen Primzahltest

1. Wie prüft man $\mathrm{ggT}(a, n) > 1$ effizient? $\Rightarrow$ euklidischer Algorithmus.
2. Wie prüft man $a^{n-1} \equiv 1 \pmod{n}$ effizient? $\Rightarrow$ schnelles modulares Potenzieren
3. Gibt es zusammengesetzte n mit $a^{n-1} \equiv 1 \pmod{n}$? $\Rightarrow$ Pseudoprimzahlen

Schnelles modulares Potenzieren

Problem: Wie prüft man $a^{n-1} \equiv 1 \pmod{n}$ effizient?

Beispiel

Wir berechnen $3^{23} \pmod{7}$.

1. Wir schreiben 23 als Summe von Zweierpotenzen:

$$23 = 16 + 7 = 16 + 4 + 3 = 16 + 4 + 2 + 1 = 2^4 + 2^2 + 2^1 + 2^0$$

2. Daraus ergibt sich

$$3^{23} = 3^{2^4+2^2+2^1+2^0} = 3^{2^4} \cdot 3^{2^2} \cdot 3^{2^1} \cdot 3^{2^0} = (((3^2)^2)^2)^2 \cdot (3^2)^2 \cdot 3^2 \cdot 3$$

3. Wir quadrieren wiederholt, und rechnen jedesmal modulo 7:

$$3^2 = 9 \equiv 2 \pmod{7} \qquad ((3^2)^2)^2 \equiv 4^2 \equiv 16 \equiv 2 \pmod{7}$$
$$(3^2)^2 \equiv 2^2 \equiv 4 \pmod{7} \qquad (((3^2)^2)^2)^2 \equiv 2^2 \equiv 4 \pmod{7}.$$

4. Wir erhalten $3^{23} \equiv ((4 \cdot 4) \cdot 2) \cdot 3 \equiv (2 \cdot 2) \cdot 3 \equiv 4 \cdot 3 \equiv 5 \pmod{7}$.

Aufgabe: Berechne $3^{33} \pmod{5}$.

Pseudoprimzahlen

Problem: Gibt es zusammengesetzte Zahlen n mit $a^{n-1} \equiv 1 \pmod{n}$?

In diesem Fall gibt der Fermatsche Primzahltest n `wahrscheinlich prim` aus, **obwohl** n **zusammengesetzt ist.**

Beispiel: Die Zahl $n = 15$ erfüllt (mit $a = 4$)

$$4^{14} \equiv 1 \pmod{15},$$

denn $4^{14} = (4^2)^7 = 16^7 \equiv 1^7 \equiv 1 \pmod{15}$.

Definition

Eine zusammengesetzte Zahl n heißt **Fermatsche Pseudoprimzahl** zur Basis a, falls

$$a^{n-1} \equiv 1 \pmod{n}.$$

Ist n eine Pseudoprimzahl zu *jeder* Basis a mit $\mathrm{ggT}(a, n) = 1$, so heißt n **Carmichael-Zahl**.

Aufgaben: Zeige, dass 341 eine Pseudoprimzahl zur Basis 2 ist.

Die kleinste Carmichael-Zahl ist übrigens 561. Es wurde erst 1994 bewiesen, dass es unendlich viele von ihnen gibt.

Der Fermatsche Primzahltest

Bespiel:

Wir wollen prüfen, ob $n = 221$ eine Primzahl ist.

Wir wählen eine zufällige Zahl $1 < a < 220$, zum Beispiel $a = 38$, und prüfen $\mathrm{ggT}(38, 221) = 1$.

Dann berechnen wir

$$a^{n-1} = 38^{220} \equiv 1 \pmod{221}.$$

Der Fermatsche Primzahltest gibt also "n `wahrscheinlich prim`" aus.

Wir wiederholen den Test mit $a = 24$ und berechnen

$$a^{n-1} = 24^{220} \equiv 81 \not\equiv 1 \pmod{221}.$$

Also muss n zusammengesetzt sein, und der Test gibt "n `zusammengesetzt`" aus.

Aufgabe: Wenden Sie den Fermatschen Primzahltest auf $n = 347921$ an.

Der Fermatsche Primzahltest

Problem beim Fermatschen Primzahltest: der Test hält **Fermatsche Pseudoprimzahlen** (manchmal) und **Carmichael Zahlen** (immer) für Primzahlen.

Durch Verfeinerung der Bedingung $a^{n-1} \equiv 1 \pmod{n}$ erhält man genauere Tests, die **weniger Pseudoprimzahlen für Primzahlen halten**.