Primzahlen im Schulunterricht – wozu?

Franz Pauer

Institut für Fachdidaktik
und
Institut für Mathematik

Universität Innsbruck

Tag der Mathematik
Graz
6. Februar 2014

Einleitung

Eine (positive) Primzahl ist eine positive ganze Zahl, die genau zwei Teiler hat.

Primzahlen kommen im Lehrplan der Sekundarstufe 1 nicht vor, wohl aber in Lehrplänen der Sekundarstufe 2.
Mit gutem Grund!

Primzahlen haben große Bedeutung für Kryptographie und Kodierungstheorie.
Diese Bedeutung erlangen sie durch „Kooperation“ mit dem erweiterten Euklidischen Algorithmus.

RSA-Verfahren

- Der Empfänger gibt zwei sehr große natürliche Zahlen n und e öffentlich bekannt.
- Der Sender will dem Empfänger die Zahl a verschlüsselt mitteilen.
- Dazu berechnet er die Zahl b, den Rest von a^e nach Division durch n.

$$b = a^e \ mod \ n$$

- Der Empfänger erhält b und berechnet für eine geeignete Zahl d den Rest von b^d nach Division durch n und erhält a !

$$b^d \ mod \ n = a$$

RSA-Verfahren

Was weiß nur der Empfänger?

- Er kennt Primzahlen p und q mit

$$n = p \cdot q\,.$$

- Er berechnet $m := (p-1) \cdot (q-1)$ und wählt e so, dass

$$ggT(e, m) = 1$$

ist.

- Er berechnet Zahlen c und d so, dass

$$m \cdot c + e \cdot d = 1$$

ist.

RSA-Verfahren

3 Fragen:

1. Die Zahl n ist bekannt. Warum kann nicht jede/r ihre Primfaktoren p und q berechnen?

2. Wie werden die ganzen Zahlen c und d (mit $m \cdot c + e \cdot d = 1$) berechnet?
   Oder: Wie löst man eine lineare Gleichung mit zwei Unbekannten ganzzahlig?

3. Warum ist für alle ganzen Zahlen a der Rest von

$$a^{e \cdot d} = a^{1-(p-1)\cdot(q-1)\cdot c} = a \cdot (a^{(p-1)\cdot(q-1)})^{-c}$$

   nach Division mit Rest durch $n = p \cdot q$ gleich a ?

Große Zahlen

2009: Faktorisierung der Zahl RSA-768 mit
232 Dezimalziffern bzw. 768 Binärziffern
Rechenzeit von mehreren hundert Computern: zweieinhalb Jahre

RSA-1024 =
135066410865995223349603216278805969938
881475605667027524485143851526510604859
533833940287150571909441798207282164471
551373680419703964191743046496589274256
239341020864383202110372958725762358509
643110564073501508187510676594629205563
685529475213500852879416377328533906109
750544334999811150056977236890927563

309 Dezimalziffern, 1024 Binärziffern
mit heutigen Methoden nicht in diesem Jahrhundert faktorisierbar

Euklidischer Algorithmus

Addition, Multiplikation, Division mit Rest auch mit Zahlen der Größe von R-1024 für Computer einfach.

Ebenso einfach: Berechnung des ggT zweier natürlicher Zahlen x und y mit dem *Euklidischen Algorithmus*.

(1) Wenn $x = y$ ist, dann ist $x = ggT(x, y)$.

(2) Solange x und y nicht gleich sind, ersetze die größere der zwei Zahlen durch die Differenz der größeren und der kleineren.

Grundidee: $ggT(x, y) = ggT(x - y, y)$.
Berechne $ggT(x - y, y)$ statt $ggT(x, y)$.

Strategie: „Wenn du ein Problem nicht lösen kannst, ersetze es durch ein einfacheres Problem mit der gleichen Lösung!“
(cf. Umformen von Gleichungen!)

Euklidischer Algorithmus, Variante

Variante des Euklidischen Algorithmus:

(1) Wenn y ein Teiler von x ist, dann ist $y = ggT(x, y)$.

(2) Solange der Rest von x nach Division durch y nicht 0 ist, ersetze die Zahl x durch ihren Rest nach Division durch y (also durch r so, dass $x = s \cdot y + r$ und $0 \leq r < y$ ist).

Grundidee: $ggT(x, y) = ggT(x - s \cdot y, y)$.
Berechne $ggT(x - s \cdot y, y)$ statt $ggT(x, y)$.

Ganzzahlige lineare Gleichungen mit zwei Unbekannten

Aufgabe: Gegeben sind ganze Zahlen u, v, w. Finde ganze Zahlen x und y so, dass x positiv ist und

$$u \cdot x + v \cdot y = w$$

ist.

- Beobachtung: wenn eine Lösung (x, y) existiert, dann muss jeder gemeinsame Teiler von u und v auch ein Teiler von w sein.
- Es genügt daher, die Gleichung

$$u \cdot x + v \cdot y = ggT(u, v)$$

zu lösen.

Ganzzahlige lineare Gleichungen mit zwei Unbekannten

- Eine Lösung von $u \cdot x + v \cdot y = u$ ist $(1, 0)$.
- Eine Lösung von $u \cdot x + v \cdot y = v$ ist $(0, 1)$.

Strategie: „Wenn du ein Problem nicht lösen kannst, dann löse zuerst einfache Probleme und versuche, aus deren Lösungen die des ursprünglichen Problems zusammenzubauen.“

Ganzzahlige lineare Gleichungen mit zwei Unbekannten

Erweiterter Euklidischer Algorithmus

- Eine Lösung von $u \cdot x + v \cdot y = u$ ist $(1, 0)$.
- Eine Lösung von $u \cdot x + v \cdot y = v$ ist $(0, 1)$.
- Eine Lösung von $u \cdot x + v \cdot y = u - m \cdot v$ ist
  $(1, 0) - m(0, 1) = (1, -m)$.
  Wir haben eine weitere Gleichung ganzzahlig gelöst!
- Wiederhole das bis zur Gleichung $u \cdot x + v \cdot y = ggT(u, v)$.

Ganzzahlige lineare Gleichungen mit zwei Unbekannten

Beispiel

- $19 \cdot x + 11 \cdot y = 19$ eine Lösung: $(1, 0)$.
- $19 \cdot x + 11 \cdot y = 11$ eine Lösung: $(0, 1)$.
- $19 \cdot x + 11 \cdot y = 19 - 11 = 8$ eine Lösung: $(1, -1)$.
- $19 \cdot x + 11 \cdot y = 11 - 8 = 3$ eine Lösung: $(-1, 2)$.
- $19 \cdot x + 11 \cdot y = 8 - 2.3 = 2$ eine Lösung: $(3, -5)$.
- $19 \cdot x + 11 \cdot y = 3 - 2 = 1$ eine Lösung: $(-4, 7)$.

Also: $19 \cdot (-4) + 11 \cdot 7 = 1$.

Ganzzahlige lineare Gleichungen mit zwei Unbekannten

Eine ganzzahlige lineare Gleichung $u \cdot x + v \cdot y = w$ hat genau dann eine ganzzahlige Lösung, wenn $ggT(u, v)$ ein Teiler von w ist.

Mit dem erweiterten Euklidischen Algorithmus kann eine Lösung (leicht) berechnet werden.

Restklassenringe

$n > 2$ natürliche Zahl
Menge $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$
Addition: $a +_n b$:= Rest von $a + b$ nach Division durch n.
Multiplikation: $a \cdot_n b$:= Rest von $a \cdot b$ nach Division durch n.

Es gelten (fast) die gleichen Rechenregeln wie für ganze Zahlen.

Kann man auch dividieren?
Zu a in $\mathbb{Z}_n$ gibt genau dann eine Zahl b in $\mathbb{Z}_n$ so, dass $a \cdot_n b = 1$ ist, wenn die lineare Gleichung $a \cdot x + n \cdot y = 1$ eine ganzzahlige Lösung hat. ($a \cdot_n x = 1$).
Also genau dann, wenn $ggT(a, n) = 1$ ist.

Restklassenkörper

Falls p eine Primzahl ist und $0 \neq a$ kleiner als p ist, ist $ggT(a, p)$ immer 1.
Also: Ist p eine Primzahl, dann ist $\mathbb{Z}_p$ ein Körper!
Dividiert wird in $\mathbb{Z}_p$ mit Hilfe des erweiterten Euklidischen Algorithmus.
In $\mathbb{Z}_p$ kann wie mit rationalen oder reellen Zahlen gerechnet werden! Gauß-Algorithmus für Systeme linearer Gleichungen anwendbar.

Wichtig für *Kodierungstheorie*.

Restklassenkörper

Man kann zeigen: Für alle Elemente z von $\mathbb{Z}_p$ ist $z^p = z$

Potenziert wird bezüglich der neuen Multiplikation, also: der Rest nach Division durch p der „gewöhnlichen“ p-ten Potenz einer Zahl ist wieder diese Zahl.

Daraus kann die Antwort auf die dritte Frage zum RSA-Verfahren abgeleitet werden.

Kriterien zur Auswahl von Algorithmen

- Welches der zwei Verfahren ist einfacher zu erklären, verlangt weniger Fachbegriffe und für welches ist die Korrektheit mit einfacheren Mitteln zu beweisen?
- Welches der zwei Verfahren ist rechnerisch effizienter, d.h. benötigt weniger Rechenaufwand, um das Ergebnis zu berechnen?
- Welches der zwei Verfahren ist leichter zu programmieren?
- Welches der zwei Verfahren kann auf andere im Schulunterricht bedeutsame Situationen angewendet werden?
- Welches der zwei Verfahren vermittelt eine grundlegende Strategie?

Euklidischer Algorithmus versus „Produkt der gemeinsamen Primfaktoren“

Berechnung des ggT wichtig zum optimalen Kürzen von Bruchzahlen

- „Theorie“ einfacher: EA
- Rechnerische Effizienz: EA (!!!!)
- Einfach zu programmieren: EA
- EA (z.B. RSA-Verfahren)
- Vermittelt Problemlösestrategie: EA

Methode des Produkts der gemeinsamen Primfaktoren legt „falsche Fährte“ , erschwert Verständnis z.B. des RSA-Verfahrens.

Danke für die Aufmerksamkeit!
http://www.uibk.ac.at/mathematik/personal/pauer/

franz.pauer@uibk.ac.at