Datenstrukturen, Algorithmen und Programmierung 2

Amin Coja-Oghlan

May 25, 2023

Lehrstuhl Informatik 2
Fakultät für Informatik

Arithmetik

Motivation

- das Rechnen mit ganzen oder rationalen Zahlen ist ein Grundbaustein vieler Algorithmen
- wir stellen die Werkzeuge dafür bereit

Arithmetik

Zahldarstellungen im Rechner

- Datentypen `int`, `unsigned int`
- Fließkommazahlen
- rationale Zahlen

Arithmetik

Elementare Rechenoperationen

- die *Darstellunglänge* einer Zahl $n \in \mathbb{N}$ ist $O(\log n)$
- Addition/Subtraktion
- Division mit Rest
- Multiplikation (!)

Arithmetik

Teilbarkeit

Seien $x, y \in \mathbb{Z}$, $x \neq 0$

- $y \mod x$ ist der Divisionsrest
- x *teilt* y, falls $y \mod x = 0$
- *Schreibweise:* $x \mid y$

Arithmetik

Größter gemeinsamer Teiler

Der ggT von $x, y \in \mathbb{Z}$, $x \neq 0$, ist die größte Zahl $z \in \mathbb{N}$, mit $z \mid x$ und $z \mid y$.

Arithmetik

Euklidischer Algorithmus $\texttt{Euclid}(a, b)$

1. falls $a < b$, vertausche a und b
2. setze $a_0 = a$, $a_1 = b$, $i = 1$.
3. solange $a_i > 0$
4. berechne $q_i \in \mathbb{Z}$, $a_{i+1} \in \{0, 1, \ldots, a_i - 1\}$, so daß $a_{i-1} = q_i a_i + a_{i+1}$.
5. erhöhe i um 1
6. gib a_{i-1} aus

Arithmetik

Satz

$\texttt{Euclid}(a, b)$ gibt $\mathrm{ggT}(a, b)$ aus und führt $O(\log(|a| + |b|))$ Division aus.

Korollar

Für je zwei Zahlen $a, b \in \mathbb{N}$ gibt es Zahlen $u, v \in \mathbb{Z}$, so daß $\mathrm{ggT}(a, b) = au + bv$.

Arithmetik

Definition

- eine Zahl $z \in \mathbb{Z} \setminus \{-1, 1\}$ heißt *irreduzibel*, falls $y \nmid z$ für alle $1 < y < |z|$.
- eine Zahl $z \in \mathbb{Z} \setminus \{-1, 0, 1\}$ heißt *Primzahl*, falls für alle $x, y \in \mathbb{Z}$ mit $z | x \cdot y$ gilt, daß $z | x$ oder $z | y$.
- mit $\mathbb{P}$ wird die Menge aller Primzahlen bezeichnet

Arithmetik

Lemma

Jede Primzahl ist irreduzibel.

Arithmetik

Lemma

Jede Zahl $z > 1$ besitzt einen irreduziblen Teiler.

Lemma

Jede irreduzibele Zahl ist eine Primzahl.

Arithmetik

Theorem

Zu jeder Primzahl $p \in \mathbb{P}$ gibt es eine Abbildung $w_p : \mathbb{N} \to \mathbb{N}_0$, so daß für jede natürliche Zahl $z \in \mathbb{N}$ gilt

$$z = \prod_{p \in \mathbb{P}} p^{w_p(z)}.$$

Diese Abbildungen w_p sind eindeutig bestimmt.

Arithmetik

Modulare Arithmetik

Seien $x, y \in \mathbb{Z}$ und $m \in \mathbb{Z} \setminus \{0\}$. Wir schreiben

$$x \equiv y \mod m \qquad \text{falls} \qquad m \mid x - y$$

Sprich: “x is kongruent zu y modulo m”.

Arithmetik

Lemma

Seien $x, y, x', y' \in \mathbb{Z}$ und $m \in \mathbb{Z} \setminus \{0\}$. Wenn

$$\begin{aligned} x &\equiv y \mod m \qquad \text{und} \qquad & x' &\equiv y' \mod m, \qquad \text{dann} \\ x + x' &\equiv y + y' \mod m \qquad \text{und} \qquad & x \cdot x' &\equiv y \cdot y' \mod m. \end{aligned}$$

Arithmetik

Lemma

Angenommen $x, y \in \mathbb{Z}$, $m, n \in \mathbb{Z} \setminus \{0\}$ und $n \mid m$. Wenn

$$x \equiv y \mod m \qquad \text{dann} \qquad x \equiv y \mod n.$$

Arithmetik

Lemma

Angenommen $x, y \in \mathbb{Z}$, $m, n \in \mathbb{Z} \setminus \{0\}$ und $\mathrm{ggT}(m, n) = 1$. Wenn

$$x \equiv y \mod m \qquad \text{und} \qquad x \equiv y \mod n \qquad \text{dann} \qquad x \equiv y \mod m \cdot n$$

Arithmetik

Chinesischer Restsatz

Angenommen $m, n \in \mathbb{N}$ sind relativ prim. Dann gibt es für je zwei ganze Zahlen x, y eine ganze Zahl z, so daß

$$z \equiv x \mod m \qquad \text{und} \qquad z \equiv y \mod n.$$

Arithmetik

Schnelles Potzenzieren

- gegeben $x \in \mathbb{Z}$ und $\ell, m \in \mathbb{N}$ suchen wir $z \in \mathbb{Z}$ mit

$$x^\ell \equiv z \mod m$$

- es wäre offenbar *nicht* effizient, x^ℓ durch ℓ-faches Multiplizieren zu berechnen

Arithmetik

Algorithmus Schnelles Potenzieren

1. Bestimme die Darstellung von ℓ im Dualsystem: $\ell = \sum_{i=0}^{k} \ell_i 2^i$
2. Sei y_0 der Divisonsrest von x durch m.
3. Für $i = 1, \ldots, k$:
4. sei y_i der Divisionsrest von y_{i-1}^2 durch m.
5. Setze $z = 1$.
6. Für $i = 0, \ldots, k$:
7. sei r der Rest von $z \cdot y_i^{\ell_i}$ durch m.
8. setze z auf den Wert r.
9. Gib z aus.

Arithmetik

Faktorisieren

- gegeben $x \in \mathbb{Z}$ ist es unser Ziel, die Primfaktorzerlegung von x zu bestimmen
- dafür ist derzeit kein effizienter Algorithmus bekannt
- wir lernen aber einen Algorithmus kennen, der für Zahlen $x = pq$ mit p, q prim und $|p - q|$ “klein” gut funktioniert

Arithmetik

Fermat-Faktorisierung

Eingabe: eine ungerade zusammengesetzte Zahl $n > 1$.

1. Setze $x = 2\lfloor\sqrt{n}\rfloor + 1$, $y = 1$, $r = \lfloor\sqrt{n}\rfloor^2 - n$.
2. Solange $r \neq 0$
3. erhöhe r um x und anschließend x um zwei
4. verringere r um y und erhöhe anschließend y um zwei
5. falls $r > 0$, gehe zurück zu (4).
6. gib die Faktorisierung $n = \left(\frac{x-y}{2}\right)\left(\frac{x+y-2}{2}\right)$ aus

Arithmetik

Zusammenfassung

- wir haben einige grundlegende Konzepte aus der Zahlentheorie kennengelernt
- modulare Arithmetik, euklidischer Algorithmus, chinesischer Restsatz
- schnelles Potzenzieren, Fermat-Faktorisierung