

Algorithmen und Datenstrukturen in C/C++

Prof. Dr. rer. nat. Peter Gerwinski

18. April 2024

Algorithmen und Datenstrukturen in C/C++

<https://gitlab.cvh-server.de/pgerwinski/ad>

- 1 Einführung
- 2 Arrays und Zeiger für Fortgeschrittene
- 3 Langzahl-Arithmetik
- 4 Kryptographie
- 5 C++
- 6 Datenorganisation
- ...



Änderungen
vorbehalten

3 Langzahl-Arithmetik

Problem: Rechnen mit ganzen Zahlen, die größer sind als das, was der Rechner normalerweise verarbeiten kann

Aufgabe: Addition langer Zahlen

- (a) Überlegen Sie sich eine Datenstruktur, um eine lange Zahl zu speichern.
- (b) Schreiben Sie eine Funktion, die zwei lange Zahlen addiert.

Lösungsansätze

- ziffernweise (z. B. Zahlen als Strings abspeichern)
- zu einer Zehnerpotenz-Basis (z. B. 1 000 000 000)
- zu einer Zweierpotenz-Basis (z. B. 2^{32})
- speziell: Registerbreite \longrightarrow Hardware-Unterstützung (in Assembler)

3 Langzahl-Arithmetik

Problem: Rechnen mit ganzen Zahlen, die größer sind als das, was der Rechner normalerweise verarbeiten kann

- Grundrechenarten (einschließlich „modulo“):
„schriftlich“ rechnen
- **binäre Exponentiation**:
Basis fortlaufend quadrieren, ggf. damit multiplizieren
Beispiel: $x^9 = ((x^2)^2)^2 \cdot x$
- Suche nach d mit $d \cdot e \bmod N = 1$:
erweiterter euklidischer Algorithmus

→ RSA

Aufgabe: RSA effizient implementieren

- Verwenden Sie den Datentyp `uint64_t` (oder Langzahl-Arithmetik)
- Für Details siehe: [ad-20240411.txt](#)

4 Kryptographie

4. $(x^2 - 1)$ Der Herr der Ringe: Manchmal ist $1 + 1 = 0$.

4. $(x^2 - 1) \cdot x$ Motivation

Man kann auch mit sehr merkwürdigen Objekten wie mit „ganz normalen“ Zahlen rechnen.

Anwendungen:

- Funktionsweise von Computern (\longrightarrow Rechnertechnik)
- Fehlererkennung
- Fehlerkorrektur
- Verschlüsselung
- Digitale Signaturen

4 Kryptographie

4. $(x^2 - 1)$ Der Herr der Ringe: Manchmal ist $1 + 1 = 0$.

4. $(x^2 - 1) \cdot (x + 1)$ Gruppen

Definition: Sei G eine Menge, $*$ eine Verknüpfung auf G . Wenn

- $\forall a, b, c \in G: (a * b) * c = a * (b * c)$ (Assoziativgesetz),
- $\exists e \in G: \forall a \in G: a * e = e * a = a$ (neutrales Element),
- $\forall a \in G: \exists a^{-1} \in G: a * a^{-1} = a^{-1} * a = e$ (inverses Element),

dann heißt $(G, *)$ eine *Gruppe*.

Definition: Sei $(G, *)$ eine Gruppe. Wenn zusätzlich

- $\forall a, b \in G: a * b = b * a$ (Kommutativgesetz),

dann heißt $(G, *)$ eine *kommutative Gruppe*.

4. $(x^2 - 1)$ Der Herr der Ringe: Manchmal ist $1 + 1 = 0$.

4. $(x^2 - 1) \cdot (x + 2)$ Ringe

Definition: Sei R eine Menge; seien $+$ und \cdot Verknüpfungen auf R . Wenn

- $(R, +)$ eine kommutative Gruppe ist,
- $\forall a, b, c \in R: (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Assoziativgesetz),
- $\forall a, b, c \in R: (a + b) \cdot c = a \cdot c + b \cdot c$ und $a \cdot (b + c) = a \cdot b + a \cdot c$ (Distributivgesetze),

dann heißt $(R, +, \cdot)$ ein *Ring*.

Definition: Sei $(R, +, \cdot)$ ein Ring. Wenn zusätzlich

- $\forall a, b \in R: a \cdot b = b \cdot a$ (Kommutativgesetz),

dann heißt $(R, +, \cdot)$ ein *kommutativer Ring*.

Definition: Sei $(R, +, \cdot)$ ein (kommutativer) Ring. Wenn zusätzlich

- ein $e \in R$ existiert, so daß für alle $a \in R$ gilt: $a \cdot e = e \cdot a = a$ (neutrales Element),

dann heißt $(R, +, \cdot)$ ein *(kommutativer) Ring mit 1*.

4. $(x^2 - 1)$ Der Herr der Ringe: Manchmal ist $1 + 1 = 0$.

4. $(x^2 - 1) \cdot (x + 3)$ Körper

Definition: Sei K eine Menge; seien $+$ und \cdot Verknüpfungen auf K . Wenn

- $(K, +, \cdot)$ ein Ring mit 1 ist und
- $(K \setminus \{0\}, \cdot)$ eine kommutative Gruppe ist,

dann heißt $(K, +, \cdot)$ ein *Körper*.

4. $(x^2 - 1)$ Der Herr der Ringe: Manchmal ist $1 + 1 = 0$.

4. $(x^2 - 1) \cdot (x + 4)$ Anwendungen

Man kann auch mit sehr merkwürdigen Objekten wie mit „ganz normalen“ Zahlen rechnen.

- innermathematisch: Man kann beweisen, daß es ab x^5 keine „ p - q -Formel“ mehr gibt und daß bestimmte Operationen mit Zirkel und Lineal unmöglich sind.
- asymmetrische Verschlüsselung, Signaturen: RSA, ElGamal, elliptische Kurven
- symmetrische Verschlüsselung: AES
- Fehlererkennung: Parität, CRC
Anwendungen: Datenübertragung, RAID
- Fehlerkorrektur: Reed-Solomon
Anwendungen: Raumsonden, optische Datenträger, ECC-RAM