

Proseminar
Effiziente Algorithmen
Kapitel 6: Zahlentheorie

Prof. Dr. Christian Scheideler
WS 2018

Zahlentheorie

- Primzahlerzeugung und -test
- Primfaktorzerlegung
- Teilbarkeit
größter gemeinsamer Teiler (ggT), kleines gemeinsames Vielfaches (kgV)
- Modulo-Arithmetik
Grundrechenarten, Lösung linearer Kongruenzen
- Diophantische Gleichungen

Primzahltest

Siehe <https://de.wikipedia.org/wiki/Primzahltest>

Primfaktorzerlegung: notorisch hartes Problem.
Einfachste Lösung bei Eingabe n (**Sieb des Eratosthenes**):
teste alle Primzahlen p von 2 bis \sqrt{n} durch.

Teilbarkeit

Bestimmung des $\text{ggT}(a,b)$:

Euklidischer Algorithmus:

```
x:=a; y:=b
while y≠0 do
  z:=x mod y; x:=y; y:=z
return(x)
```

Bestimmung des $\text{kgV}(a,b)$:

$$a \cdot b = \text{ggT}(a,b) \cdot \text{kgV}(a,b)$$

Teilbarkeit

- Gegeben: $a, b \in \mathbb{N}$
- Gesucht: $d = \text{ggT}(a, b)$ und $x, y \in \mathbb{Z}$ mit $d = x \cdot a + y \cdot b$

Erweiterter Euklidischer Algorithmus:

```
a0 := a; a1 := b
x0 := 1; y0 := 0; x1 := 0; y1 := 1
while ai+1 ≠ 0 do
  qi+1 := ai div ai+1
  ai+2 := ai mod ai+1
  xi+2 := xi - qi+1 · xi+1
  yi+2 := yi - qi+1 · yi+1
  i := i + 1
d := ai; x := xi; y := yi
return(d, x, y)
```

Modulo-Arithmetik

- Gegeben: $m, a, n \in \mathbb{N}$
- Gesucht: b mit $b = a^n \bmod m$

Algorithmus:

```
b:=1; c:=a; e:=n
while e>0 do
  if odd(e) then b:=b·c mod m
  e:=e div 2
  c:=(c·c) mod m
return b
```

Modulo-Arithmetik

- Gegeben: $a, b, n \in \mathbb{N}$
- Gesucht: alle Lösungen x von $a \cdot x = b \pmod{n}$
- Sei $\text{ggT}(a, n) = d$. Dann hat die Kongruenz eine Lösung genau dann wenn $d \mid b$.
- Sei r eine spezielle Lösung. Dann besteht die Lösungsmenge aus allen $x = r + t \cdot n/d$, $t \in \mathbb{Z}$

Verfahren zur Lösung von $a \cdot x = b \pmod{n}$ mit $\text{ggT}(a, n) = d$:

1. Finde (mithilfe des Euklidischen Algorithmus) Zahlen y und z , so dass $a \cdot y + n \cdot z = d$.
2. Setze $x := y \cdot b$. Dann ist $a \cdot x = b \pmod{n}$.

Diophantische Gleichungen

- Diophantische Gleichungen sind Formeln, in denen die Variablen ganze Zahlen sein müssen.
- Das Problem, diophantische Gleichungen zu lösen, ist bekanntermaßen sehr hart.
- Aber lineare diophantische Gleichungen sind mithilfe von Erweiterungen des Euklidischen Algorithmus lösbar.

Probleme

- 10104: Euclid Problem
- 10042: Smith Numbers
- 10090: Marbles
- 10110: Light, More Light
- 10006: Carmichael Numbers
- 10139: Factovisors
- 106: Fermat vs. Pythagoras

Hausaufgabe:

- 10168: Summation of Four Primes