Proseminar
Effiziente Algorithmen

Kapitel 6: Zahlentheorie

Prof. Dr. Christian Scheideler

WS 2017

Zahlentheorie

- Primzahlerzeugung und -test
- Primfaktorzerlegung
- Teilbarkeit
  größter gemeinsamer Teiler (ggT), kleines gemeinsames Vielfaches (kgV)
- Modulo-Arithmetik
  Grundrechenarten, Lösung linearer Kongruenzen
- Diophantine 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 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 kgV(a,b):

$$a \cdot b = ggT(a,b) \cdot kgV(a,b)$$

Teilbarkeit

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

Erweiterter Euklidischer Algorithmus:

$a_0 := a$; $a_1 := b$
$x_0 := 1$; $y_0 := 0$; $x_1 := 0$; $y_1 := 1$
while $a_{i+1} \neq 0$ do
  $q_{i+1} := a_i$ div a_{i+1}
  $a_{i+2} := a_i$ mod a_{i+1}
  $x_{i+2} := x_i - q_{i+1} \cdot x_{i+1}$
  $y_{i+2} := y_i - q_{i+1} \cdot y_{i+1}$
  $i := i+1$
$d := a_i$; $x := x_i$; $y := y_i$
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 $a \cdot x = b \bmod n$

- Sei $ggT(a,n)=d$. Dann hat die Kongruenz eine Lösung genau dann wenn $d|b$.
- 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 $a \cdot x = b \bmod n$ mit $ggT(a,n)=d$:

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 $a \cdot x = b \bmod n$.

Diophantine Gleichungen

- Diophantine Gleichungen sind Formeln, in denen die Variablen ganze Zahlen sein müssen.
- Das Problem, diophantine Gleichungen zu lösen, ist bekanntermaßen sehr hart.
- Aber lineare diophantine 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