Wiederholung

Größte gemeinsame Teiler

- Satz von Bezout:
  - $ggT(a,b) = \min\{k \in \mathbb{N} \mid k = ax + by, x,y \in \mathbb{Z}\}$
- Satz zur Teilerfremdheit:
  - $ggT(a,p)=ggT(b,p)=1 \Rightarrow ggT(ab,p)=1$
- Fundamentalsatz der Arithmetik
  - Jedes n besitzt eine eindeutige Primfaktorzerlegung
- ggT-Satz:
  - $ggT(a,b) = ggT(b, a \bmod b)$
- Euklidischer Algorithmus

Euklidischer Algorithmus (300 v. Chr.)

Algorithmus Euklid
Eingabe: a,b $\in \mathbb{N}$

1. if (b=0) then return a;
2. else return Euklid(b, a mod b)

Ausgabe: ggT(a,b)

Korrektheit:

- Schritt 1.: ggT(a,0) = a.
- Schritt 2.: Folgt aus ggT-Satz.

Laufzeit des Euklidischen Algorithmus

Fibonacci-Zahlen:

- F_0:=0, F_1 := 1
- F_i := F_{i-1}+F_{i-2} für i $\geq$ 2.

Satz: Sei a>b und sei k die Anzahl von Rekursionen in Euklid(a,b). Dann gilt a $\geq$ F_{k+2} und b $\geq$ F_{k+1}.

Induktion über k:

- IA: k=1: b$\geq$1= F_2
  a > b, d.h. a $\geq$ 2=F_3
- IS: k-1 $\rightarrow$ k:
  - Euklid(a,b) ruft Euklid(b, a mod b) auf.
  - Euklid(b, a mod b) benötigt k-1 Aufrufe, d.h.
    b $\geq$ F_{k+1} und (a mod b) $\geq$ F_k.
  - b + (a mod b) = b + (a - $\lfloor$a/b$\rfloor$b) $\leq$ a (wegen a>b folgt $\lfloor$a/b$\rfloor$ $\geq$ 1)
    $\Rightarrow$ a $\geq$ b + (a mod b) $\geq$ F_{k+1} + F_k = F_{k+2}

Logarithmische Laufzeit

Korollar: Sei a>b und b<F_{k+1}. Dann benötigt Euklid(a,b) weniger als k rekursive Aufrufe.

Es gilt: $F_k = \Theta(\phi^k)$, wobei $\phi = \frac{1+\sqrt{5}}{2}$ der goldene Schnitt ist.
$\Rightarrow$ k = $\mathcal{O}$(log b) rekursive Aufrufe

- Wegen a>b gilt $\mathcal{O}$(log b) = $\mathcal{O}$(log a) rekursive Aufrufe.
- Multiplikation/Division mit Operanden der Bitlänge $\mathcal{O}$(log a): Zeit $\mathcal{O}(\log^2 a)$
- Insgesamt: $\mathcal{O}(\log^3 a)$

- Man beachte: a,b werden sukzessive kleiner.
- Exakte Analyse liefert $\mathcal{O}(\log^2 a)$.

Fibonacci-Zahlen sind worst-case

Wählen $b=F_k<F_{k+1}$.

$$\begin{aligned}\text{Euklid}(F_{k+1},F_k) &= \text{Euklid}(F_k, F_{k+1} \bmod F_k) = \text{Euklid}(F_k, F_{k-1})\\ &= \text{Euklid}(F_{k-1}, F_{k-2})\\ &\dots\\ &= \text{Euklid}(F_3, F_2) = \text{Euklid}(2,1)\\ &= \text{Euklid}(1,0)\end{aligned}$$

Man benötigt genau k-1 rekursive Aufrufe

Erweiterter Euklidischer Algorithmus

Erweiterter Euklidischer Algorithmus (EEA)
Eingabe: a,b $\in \mathbb{N}$

1. If (b=0) return (a,1,0)
2. (d‘,x‘,y‘) $\leftarrow$ EEA(b, a mod b)
3. (d,x,y) $\leftarrow$ (d‘,y‘,x‘-$\lfloor a/b \rfloor$y‘)

Ausgabe: d = ggT(a,b) = xa+yb

Korrektheit:

- Schritt1.: b=0: d = a = ggT(a,0) = 1*a + 0*b
- Schritt2.: d‘ = x‘b + y‘(a mod b)
  und d‘ = ggT(b, mod a) = ggT(a,b) = d (ggT-Satz)
  Schritt3.: $\Rightarrow$ d = x‘b + y‘(a-$\lfloor a/b \rfloor$b) = y‘a + (x‘-$\lfloor a/b \rfloor$y‘)b = xa + yb

Laufzeit: $\mathcal{O}(\log^2 a)$ analog zu Euklid(a,b)

Beispiel ggT(15,11)

a	b	⌊ a/b ⌋	x	y
15	11	1	3	-4
11	4	2	-1	3
4	3	1	1	-1
3	1	3	0	1
1	0	-	1	0

Alternative Schreibweise:

15 - 1*11 = 4 1 = 11 + 3*(15-1*11) = 3*15-4*11

11 – 2* 4 = 3 1 = 4 – 1*(11-2*4) = -11+3*4

4 – 1* 3 = 1 1 = 4 – 1*3

3 - 3* 1 = 0

Abelsche Gruppen

Def: Eine abelsche Gruppe ist ein Tupel $(G, \circ)$ bestehend aus einer Menge G und einer Verknüpfung $\circ$ mit

1. Abgeschlossenheit: $\circ : G \times G \to G, (a,b) \mapsto a \circ b$
2. Kommutativität: $a \circ b = b \circ a$
3. Assoziativität: $(a \circ b) \circ c = a \circ (b \circ c)$
4. Neutrales Element: $\exists!\ e: a \circ e = a$ für alle $a \in G$.
5. Inverses Element:
   1. Schreibweise multiplikativ: $\exists!\ a^{-1}: a \circ a^{-1} = e$ für alle $a \in G$.
   2. Schreibweise additiv : $\exists!\ -a : a \circ -a = e$ für alle $a \in G$.

Vereinfachte Schreibweise: G statt $(G, \circ)$

Beispiele für Gruppen

- $(\mathbb{Z},+)$ ist additive Gruppe:
  - Neutrales Element: 0
  - Inverses von $a \in \mathbb{Z}$: -a
- $(\mathbb{Q} \setminus \{0\}, *)$ ist multiplikative Gruppe:
  - Neutrales Element: 1
  - Inverses von $a/b \in \mathbb{Q} \setminus \{0\}$: b/a
- $(\mathbb{Z}, *)$ ist keine Gruppe:
  - 2 besitzt kein Inverses in $\mathbb{Z}$

Betrachten nun Beispiele für endliche Gruppen.

Die additive Gruppe $(\mathbb{Z}_m,+)$

Satz: Die Menge $\mathbb{Z}_m$ ist zusammen mit der Addition modulo m eine additive Gruppe.

- Abgeschlossenheit: $\mathbb{Z}_m \times \mathbb{Z}_m \rightarrow \mathbb{Z}_m$

  Sei a+b = q*m+r, mit $0 \leq$ r <m. Dann gilt:

  a+b = r mod m mit r $\in \mathbb{Z}_m$
- Kommutativität und Assoziativität:
  - Folgen aus Kommutativität und Assoziativität der Addition über $\mathbb{Z}$.
- Neutrales Element: $0 \in \mathbb{Z}_m$: a+0 = a mod m
- Inverses von a:

  -a = (m-a) $\in \mathbb{Z}_m$ für a $\neq$ 0: a+(m-a) = m = 0 mod m

  -0 = 0 $\in \mathbb{Z}_m$ für a=0 : 0+0 = 0 mod m

Definition $\mathbb{Z}_n^*$.

Def.: Sei n $\in \mathbb{N}$.

- **$\mathbb{Z}_n^*$:= {a $\in \mathbb{Z}_n$ | ggT(a, n)=1}**
- **Eulersche phi-Funktion: ϕ(n):= $|\mathbb{Z}_n^*|$**

Beispiele:

- Sei p=n prim.
  - $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} = \{1,2,\ldots,p-1\}$
  - $\phi(p) = |\{1,2,\ldots p-1\}| = p-1$
- Sei n=p*q mit p,q prim (RSA-Modul)
  - $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0,p,2p,\ldots,(q-1)p,q,2q,\ldots,(p-1)q)$
  - $\phi(n) = |\mathbb{Z}_n^*| = n-1-(q-1)-(p-1) = n-p-q+1 = (p-1)(q-1)$

Die multiplikative Gruppe $\mathbb{Z}_n^*$

Satz: $\mathbb{Z}_n^*$ ist zusammen mit der Multiplikation modulo n eine multiplikative Gruppe.

- Abgeschlossenheit: $\mathbb{Z}_n^* \times \mathbb{Z}_n^* \to \mathbb{Z}_n^*$
  - Satz zur Teilerfremdheit: Seien $a,b \in \mathbb{Z}_n^*$, d.h. ggT(a,n)=ggT(b,n)=1.
    $\Rightarrow$ ggT(a*b, n)=1=ggT(a*b mod n, n) (ggT-Satz), d.h. a*b mod n $\in \mathbb{Z}_n^*$
- Kommutativität und Assoziativität:
  - Folgen aus Kommutativität/Assoziativität der Multiplikation über $\mathbb{Z}$.
- Neutrales Element: $1 \in \mathbb{Z}_n^*$: a*1 = a mod n für alle $a \in \mathbb{Z}_n^*$
- Inverses von $a \in \mathbb{Z}_n^*$:
  - Satz von Bezout: 1 = ggT(a,n) = ax + ny für $x,y \in \mathbb{Z}$.
    OBdA $x \in \mathbb{Z}_n$, denn 1 = a(x+kn) + n(y-ak) für alle $k \in \mathbb{Z}$
    Es gilt ax = 1 – ny = 1 mod n, d.h. $x = a^{-1} \in \mathbb{Z}_n$.
    Ferner gilt $x \in \mathbb{Z}_n^*$, da xa + ny = 1 = ggT(x,n) (Satz von Bezout).