Wiederholung

Die schnelle Fouriertransformation (FFT)

- Umwandlung in Point-Value Form
  - n-te Einheitswurzeln
  - DFT(a, ω): Auswerten von a an n-ten Einheitswurzeln
  - FFT: Divide-and-conquer in $\mathcal{O}$(n logn)
    - Polynome a_g, a_u mit Grad n/2
    - Auswerten an n/2 vielen Stellen
- Umwandlung in Koordinatenform
  - Inverse DFT: $DFT_n^{-1}(y, \omega) = 1/n\ DFT(y, \omega^{-1})$

Bsp. FFT: a(x)*b(x) = (x+2)*(3x+4)

- $DFT_4(a, \omega)$, $DFT_4(b, \omega)$:
  - Auswerten von a(x), b(x) an (1, i, -1, -i):
  - $DFT_4(a, \omega) = (3, i+2, 1, 2-i)$
  - $DFT_4(b, \omega) = (7, 4+3i, 1, 4-3i)$
- $DFT_4(c, \omega) = (21, 5+10i, 1, 5-10i)$
- $DFT_4^{-1}(c, \omega) = \frac{1}{4} * DFT_4(c, \omega^{-1})$
  - Auswerten von $21+(5+10i)x+x^2+(5-10i)x^3$ an (1, -i, -1, i):
  - $\frac{1}{4} * DFT_4(c, \omega^{-1}) = \frac{1}{4} * (32, 40, 12, 0) = (8, 10, 3, 0)$

$$\Rightarrow a(x)*b(x) = 8 + 10x + 3x^2$$

Körper

Def: Sei K eine Menge. (K,+,*) ist ein Körper falls

- **(K1): (K,+) ist additive abelsche Gruppe mit neutralem Element 0.**
- **(K2): (K\{0},*) ist multiplikative abelsche Gruppe mit neutralem Element 1.**
- **(K3): Distributivität:**
  - **a*(b+c) = a*b + a*c für alle a,b,c $\in$ K**

Beispiele:

- $\mathbb{Q}$ ist ein Körper
- $\mathbb{R}$, $\mathbb{C}$ sind Körper
- $\mathbb{Z}$ ist kein Körper: 2 besitzt kein multiplikatives Inverses.
  - Def. Ring: (K1)-(K3), außer dass Existenz von multiplikativen Inversen gefordert wird.
  - ($\mathbb{Z}$,+,*) ist ein Ring.

Nullteilerfreiheit in Körpern

Lemma: Sei K ein Körper. Dann gilt für alle a $\in$ K:
a*0 = 0*a = 0.

Beweis: a*0 = a*(0+0) = a*0 + a*0
$\Rightarrow$ a*0 = 0

Satz: Sei K ein Körper. Dann gilt für alle a,b $\in$ K:
a*b = 0 $\Rightarrow$ a=0 oder b=0.

- Sei a*b = 0 und a$\neq$ 0
  $\Rightarrow$ b = 1*b = a^{-1}*a*b = a^{-1}*0 = 0.

Endliche Körper

Satz: Sei p prim. Dann ist $\mathbb{F}_p = (\mathbb{Z}_p,+,*)$ ein Körper mit p Elementen.

Beweis:

- $(\mathbb{Z}_p,+)$ ist eine additive Gruppe.
- $(\mathbb{Z}_p \setminus \{0\},*) = (\mathbb{Z}_p^*,*)$ ist eine multiplikative Gruppe.
- Distributivität: Folgt aus Distributivität über $\mathbb{Z}$.

Polynome über K

- Sei K ein Körper und $a(x) \in K[x]$, d.h.
  - $a(x) = \sum_i a_i x^i$ mit $a_i \in K$.

- Erinnerung Euklidische Division für Polynome:
  - Für $a(x),b(x) \in K[x]$, $b \neq 0$ gilt:
    $\exists\ q(x),r(x) \in K[x]$ mit $a(x) = q(x)*b(x) + r(x)$ mit $grad(r)<grad(b)$
  - Beweis geführt für $K = \mathbb{Q}$. Gilt analog für beliebige K.

- x_0 ist Nullstelle von $a(x) \Leftrightarrow a(x_0)=0$.

Anzahl Nullstellen eines Polynoms

Satz: Sei K ein Körper und $p(x) \in K[x]$, $p(x) \neq 0$ mit n=grad(p). Dann hat p(x) höchstens n Nullstellen.

Induktion über n:

- IA: Sei n=0. Dann ist $p(x)=a$ mit $a \neq 0$.
  D.h. p(x) hat keine Nullstelle.
- IS: n-1 $\rightarrow$ n.
  - Fall 1: p(x) hat keine Nullstelle und damit höchstens n.
  - Fall 2: Sei x_0 Nullstelle von p(x).
    - Euklidische Division: $\exists$ q(x), r(x) mit
      $p(x) = q(x)*(x-x_0) + r(x)$ mit grad(r)<1.
    - Auswerten an Nullstelle x_0 liefert:
      $0 = p(x_0) = q(x_0)*(x_0-x_0) + r(x_0) = q(x_0)*0 + r(x_0) = r(x_0)$
      $\Rightarrow r(x_0) = 0$.
    - D.h. $p(x) = q(x)*(x-x_0)$ mit grad(q)=n-1
    - Nach IV hat q(x) höchstens n-1 Nullstellen und damit p(x) höchstens n Nullstellen.

Ordnungen und Teilbarkeit

Satz: Sei G eine multiplikative Gruppe. Dann gilt für alle $a \in G$, $k \in \mathbb{N}$:

$$\mathbf{a^k = 1 \Leftrightarrow ord(a) \mid k}$$

„$\Rightarrow$“:

- $a^k = 1 \Rightarrow k \geq ord(a)$.
- Ann.: $ord(a) \nmid k$

  $\Rightarrow k = q*ord(a) + r$ mit $r<ord(a)$

  Aber $1 = a^k = a^{q*ord(a)+r} = 1^q * a^r = a^r$ mit $r<ord(a)$

  (Widerspruch zur Minimalität der Ordnung)

„$\Leftarrow$“:

- Sei $k = ord(a)*q$.

  $\Rightarrow a^k = (a^{ord(a)})^q = 1$.

Multiplikativität der Ordnung

Lemma: Sei G eine abelsche Gruppe und a,b $\in$ G mit ggT(ord(a), ord(b))=1. Dann gilt: ord(ab) = ord(a)*ord(b).

- $(ab)^{ord(a)*ord(b)} = (a^{ord(a)})^{ord(b)} * (b^{ord(b)})^{ord(a)} = 1$
  $\Rightarrow$ ord(ab) | ord(a)*ord(b)
- Ann: ord(ab)*k = ord(a)*ord(b) mit k>1
  - ObdA k‘=ggT(ord(a),k)>1 mit k‘ | k.
    $\Rightarrow 1 = (ab)^{ord(a)*ord(b)/k‘}$
    $= a^{ord(a)*ord(b)/k‘} * (b^{ord(b)})^{ord(a)/k‘} = a^{ord(a)*ord(b)/k‘}$
    $\Rightarrow$ ord(a) | ord(a)/k‘*ord(b) (ggT(ord(a), ord(b)) = 1)
    $\Rightarrow$ ord(a) | ord(a)/k‘ (Widerspruch wegen k‘>1)

Elementordnung | max. Elementordnung

Satz: Sei G eine endliche abelsche Gruppe und a ein Element mit maximaler Ordnung. Dann gilt für alle b $\in$ G:

ord(b) | ord(a).

Ann: ord(b) $\nmid$ ord(a), d.h. ggT(ord(a),ord(b)) < ord(b) (*)

- ord(ab) = ord(a)*ord(b)/ggT(ord(a),ord(b)) > ord(a) (wegen (*))
  (Widerspruch zur Maximalität von ord(a))