Wiederholung

- Körper K
  - $(K,+)$, $(K\backslash\{0\},*)$ abelsche Gruppen, Distributivität
  - Nullteilerfrei
  - $\mathbb{F}_p = (\mathbb{Z}_p,+,*)$ ist endlicher Körper für primes p
  - $f(x) \in K[x]$ mit grad(f)=n hat höchstens n Nullstellen
- Eigenschaften von multiplikativen Gruppen
  - $a^k=1 \Leftrightarrow \mathrm{ord}(a) \mid k$
  - ord(ab) = ord(a)*ord(b) für ggT(ord(a), ord(b))

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)
  $\Rightarrow \exists$ Primzahl p und ein i $\in \mathbb{N}_0$ mit
  p^{i+1} | ord(b) und p^i | ord(a) und $p^i \nmid$ ord(a)
  Definiere a' = a^{p^i} und b' = $b^{ord(b)/p^{i+1}}$.
  $\Rightarrow$ ord(a') = ord(a)/p^i und ord(b')=p^{i+1}.

- Wegen p $\nmid$ ord(a') gilt ggT(ord(a'), ord(b')) = 1.
  $\Rightarrow$ ord(a'b') = ord(a)*p > ord(a)
  (Widerspruch zur Maximalität von ord(a))

K^* ist zyklisch.

Satz: Sei K ein endlicher Körper. Dann ist die multiplikative Gruppe $(K \backslash \{0\},*)$ zyklisch.

- Sei a Element mit maximaler Ordnung in $K^* = K \backslash \{0\}$.
  - Satz von Lagrange: ord(a)| |K*|.
- Betrachten Polynom $p(x)=x^{ord(a)}-1$.
  - Wegen ord(b) | ord(a) für alle $b \in K^*$ gilt p(b)=0.
  - Damit hat p(x) genau $|K^*|$ viele Nullstellen.
  - Jedes Polynom vom Grad ord(a) hat höchstens ord(a) Nullstellen.

    $\Rightarrow |K^*| \leq ord(a)$.

    $\Rightarrow ord(a) = |K^*|$

Anzahl der Generatoren

Satz: Sei K ein Körper mit q Elementen. Dann hat K genau ϕ(q-1) viele Generatoren.

- K^* ist zyklisch, besitzt also einen Generator a:
  - $K = \{a, a^2, a^3, \ldots, a^{|K^*|}\}$
- Zeigen a^j Generator $\Leftrightarrow$ ggT(j, $|K^*|$) = 1 (Übungsaufgabe)
  - Es gilt $|\{j \in \mathbb{Z}_{\{|K^*|\}} \mid \mathrm{ggT}(j, |K^*|)=1\}| = \phi(|K^*|) = \phi(q-1)$.

Beispiel: $\mathbb{Z}_{11}^*$

- $(\mathbb{Z}_{11}^*,*)$ ist zyklisch und hat $\phi(10)=(2-1)(5-1)=4$ Generatoren.
- Man beachte: a Generator $\Leftrightarrow a^{\phi(N)/k} \neq 1$ für alle Teiler k von $\phi(N)$.
- 2 ist Generator, da $2^2=4$ und $2^5=(-1)$.
- $\mathbb{Z}_{10}^* = \{1,3,7,9\}$.
- Damit sind $2^3=8$, $2^7=7$ und $2^9=6$ ebenfalls Generatoren:

Algorithmus zum Finden von Generatoren in $\mathbb{Z}_p^*$
(bei bekannter Primfaktorzerlegung von $\phi(p-1)$)

1. Wähle $a \in \mathbb{Z}_p^*$ zufällig.
2. Für alle Teiler k von $\phi(p-1)$: Falls $a^{\phi(p-1)/k} = 1$, gehe zu Schritt 1.

Erwartete Anzahl von Iterationen: $p-1/\phi(p-1)$.

Teilbarkeitsbegriff für Polynome

Sei K ein Körper und f(x), g(x), π(x) $\in$ K[x].

- (K[x],+,*) ist ein Ring.
- Benötigen multiplikative Inverse für Körpereigenschaft

- g(x) | f(x) $\Leftrightarrow$ $\exists$ h(x)$\in$ K[x]: g(x) * h(x) = f(x)

- f(x) = g(x) mod π(x) $\Leftrightarrow$ π(x) | f(x) - g(x)
  - Erhalten analog zu den ganzen Zahlen Äquivalenzklassen.
  - Repräsentanten der Aquivalenzklassen bei Reduktion mit π(x):
    R = { f(x) | grad(f) < grad(π) }
  - Sei K endlicher Körper mit p Elementen und grad(π)=n: |R|=p^n.
- Notation K[x]/(π(x)).

- ggT(f(x),g(x)) = d(x) $\Leftrightarrow$ d(x) hat maximalen Grad unter allen Teilern von f(x), g(x)

Erweiterter Euklidischer Algorithmus

Erweiterter Euklidischer Algorithmus (EEA) für Polynome

Eingabe: a(x),b(x) $\in \mathbb{K}$**[x]**

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

Ausgabe: d(x) = ggT(a(x),b(x)) = r(x)a(x)+s(x)b(x)

Korrektheit: analog zu $\mathbb{N}$.

Beispiel ggT(x^3+2x^2-1, x^2+x) in $\mathbb{Z}_3[x]$

a	b	$\lfloor a/b \rfloor$	r	s
x^3+2x^2-1	x^2+x	$x+1$	1	$-x-1$
x^2+x	$2x-1$	$2x+2$	0	1
$2x-1$	0	-	1	0

- ggT(a(x), b(x)) = 2x-1
  - Beachte: ggT(a,b) eindeutig bis auf Multiplikation mit $a \in \mathbb{Z}_3^*$:
    2*(2x-1) = x+1 ist ebenfalls Teiler von a(x),b(x),
    denn (-1) ist Nullstelle von beiden Polynomen.

- ggT(a(x),b(x)= r(x)*a(x) + s(x)*b(x)
  $= x^3+2x^2-1 - (x+1)(x^2+x) = -x-1 = 2x-1$

Irreduzible Polynome

Sei $\pi(x)=\pi_1(x)*\pi_2(x) \in K[x]$ mit $1 \leq \mathrm{grad}(\pi_1(x)), \mathrm{grad}(\pi_2(x)) < \mathrm{grad}(\pi(x))$.
Dann gilt $\pi_1(x)*\pi_2(x) = 0$ in $K[x]/(\pi(x))$.

$\Rightarrow$ $K[x]/(\pi(x))$ ist kein Körper für nicht-trivial zerlegbare $\pi(x)$.

Def: Sei K ein Körper, $\pi(x) \in K[x]$.
$\pi(x)$ heisst irreduzibel über K genau dann, wenn
$\pi(x) = \pi_1(x)*\pi_2(x)$ mit $\pi_1(x),\pi_2(x) \in K[x] \Rightarrow \mathrm{grad}(\pi_1)=0$ oder $\mathrm{grad}(\pi_2)=0$.

Andernfalls heisst $\pi(x)$ reduzibel.

Beispiel x^2+1

Polynom $f(x) = (x^2+1)$:

- Irreduzibel über $\mathbb{R}$
  - $f(x) > 0$ für alle $x \in \mathbb{R}$
- Reduzibel über $\mathbb{C}$
  - $f(x) = (x+i)(x-i)$
- Irreduzibel über $\mathbb{Z}_3$
  - 0,1,2 sind keine Nullstellen von p(x) in $\mathbb{Z}_3$.
- Reduzibel über $\mathbb{Z}_2$
  - $f(x) = (x+1)(x+1)$

Galoiskörper

Satz: Sei K ein Körper mit p Elementen und $\pi(x) \in K[x]$ irreduzibel über K mit Grad n. Sei $q=p^n$. Dann ist $\mathbb{F}_{p^n} = \mathbb{F}_q = K[x]/(\pi(x))$ ein Körper mit q Elementen.
$\mathbb{F}_q$ wird oft auch mit GF(q) bezeichnet.

- $(K[x]/(\pi(x)),+)$ abelsche Gruppe
  - Definiere $H=\{t(x)*\pi(x) \mid t(x) \in K[x]\}$.
  - H ist Untergruppe von K[x].
  - Faktorgruppe $K[x]/H \cong K[x]/(\pi(x))$
- $(K[x]\backslash\{0\}/(\pi(x)),*)$ abelsche Gruppe
  - Abgeschlossenheit: Seien $f(x), g(x) \in K[x]\backslash\{0\}$.
    Ann.: $f(x)*g(x) = 0 \bmod \pi(x)$
    $\Rightarrow \pi(x) \mid f(x)*g(x) \Rightarrow \pi(x) \mid f(x)$ oder $\pi(x) \mid g(x)$ (Widerspruch: $f,g \neq 0$)
  - Berechnen von Inversen: EEA für Polynome.
- Distributivgesetz: nachrechnen

Beispiel $\mathbb{F}_4$

- Körper $\mathbb{F}_{2^2} = \mathbb{F}_4$:
  - Körpererweiterung des Grundkörpers $\mathbb{F}_2$
  - $\pi(x) = (x^2+x+1)$ ist irreduzibel über $\mathbb{F}_2$, wegen $\pi(0) = \pi(1) = 1$.

- Elemente von $\mathbb{F}_4$: $\{0,1,x,x+1\}$
  - Inverses von x: EEA$(x,\pi(x))$ liefert $1*(x^2+x+1) + x*(x+1) = 1$

    $\Rightarrow x*(x*1) = 1 \bmod \pi(x)$
  - Alternativ: Löse Gleichungssystem in a,b im $\mathbb{F}_2[x]/(x^2+x+1)$:

    $$\begin{aligned}(ax+b)*(x+1) = 1 &\Leftrightarrow (ax^2+(a+b)x+b) = 1\\ &\Leftrightarrow (a(x+1)+(a+b)x+b) = 1\\ &\Leftrightarrow (bx+(a+b))=1\end{aligned}$$

    $\Rightarrow$ b=0 und a+b=1, d.h. a=1. D.h. x ist das Inverse von x+1.

- $\mathbb{F}_4$ hat $\phi(3)=2$ Generatoren: x und x+1.
  - $x^2=x+1$, $x^3=1$ und $(x+1)^2=x$, $(x+1)^3=1$

Damit bleibt mir nur folgender Wunsch …

Ein frohes Fest und einen guten Rutsch!