# 14. Vorlesung. – Wiederholung.

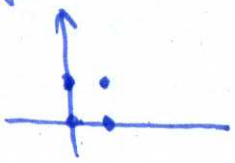
**Satz (Chevalley & Warning)** Es seien $F$ ein endl. Körper der Charakteristik $p$ und $P_1, \dots, P_m \in F[X_1, \dots, X_n]$ Polynome. Wenn $\sum_{i=1}^{m} \deg(P_i) < n$, dann ist die Anzahl der gem. Nullstellen von $P_1, \dots, P_m$ durch $p$ teilbar.

**Satz (Olson)** $D(\mathbb{F}_p^n) = n(p-1)+1$

**Satz (Erdős, Ginzburg, Ziv)** Für alle $A \subseteq \mathbb{Z}$ mit $|A| = 2n-1$ gibt's $B \subseteq A$ mit $|B| = n$ und $n \mid \sum_{b \in B} b$.

**Kemnitz - Vermutung 9.17** Jede Menge $A \subseteq \mathbb{Z}^2$ mit $|A| = 4n-3$ hat eine Teilmenge $B \subseteq A$ mit $|B| = n$, deren Schwerpunkt in $\mathbb{Z}^2$ liegt.

**Bemerkungen. 9.18** (1) Die Zahl $4n-3$ ist sicher optimal, denn: Wenn $A$ je $n-1$ Punkte enthält, die zu $(0,0), (1,0), (0,1), (1,1)$ kongruent sind, gibt's keine solche Teilmenge.



(2) Wie im Beweis des Satzes von Erdős, Ginzburg und Ziv genügt es, den Fall $n$ zu behandeln, dass $n$ eine Primzahl ist.

(3) Der Fall $n = 2$ ist trivial, denn: Wegen $|(\mathbb{Z}/2\mathbb{Z})^2| = 4$ gibt's unter $4 \cdot 2 - 3 = 5$ Punkten stets 2, die modulo $(2\mathbb{Z})^2$ kongruent sind. Diese tun's.

(4) Kemnitz löste außerdem die Fälle $n = 3, 5, 7$.

**Notation.**

- $p$ Primzahl
- Ist $X \subseteq \mathbb{Z}^2$ endlich, so schreiben wir $\sum X$ für $\sum_{x \in X} x$.
- Ist außerdem $n \in \mathbb{N}$, dann schreiben wir $(n, X)$ für die Anzahl der $Y \subseteq X$ mit $|Y| = n$ und $\sum Y \equiv (0,0) \pmod{p}$.

**Lemma 9.19.** Für alle $X \subseteq \mathbb{Z}^2$ mit $|X| \in \{3p-2, 3p-1\}$ gilt

$$1 - (p, X) + (2p, X) \equiv 0 \pmod{p}$$

**Beweis.** Schreibe $X = \{(a_i, b_i) : i \in [|X|]\}$ und betrachte das Gleichungssystem

$$\sum_{i=1}^{|X|} Z_i^{p-1} = 0$$

$$\sum_{i=1}^{|X|} a_i Z_i^{p-1} = 0$$

$$\sum_{i=1}^{|X|} b_i Z_i^{p-1} = 0.$$

Da $|X| > 3(p-1)$ ist die Anzahl der Lösungen (in $\mathbb{F}_p^{|X|}$) durch $p$ teilbar.

Andererseits ist die Anzahl der Lösungen

$$1 + (p-1)^p (p, X) + (p-1)^{2p} (2p, X).$$

□

**Lemma 9.20.** Für alle $y \subseteq \mathbb{Z}^2$ mit $|y| = 4p-2$ ist

$$2 - (p, y) + (3p, y) \equiv 0 \pmod{p}.$$

**Beweis.** Wie im vorigen Beweis zeigt man

$$1 - (p, y) + (2p, y) - (3p, y) \equiv 0 \pmod{p} \quad \dots\dots (1)$$

Außerdem folgt aus Lemma 9.19

$$\sum_{x \subseteq y,\, |x| = 3p-2} \left( 1 - (p, x) + (2p, x) \right) \equiv 0 \pmod{p},$$

d.h.

$$\binom{4p-2}{p} - \binom{3p-2}{p} (p, y) + \binom{2p-2}{p} (2p, y) \equiv 0 \pmod{p}.$$

Nun ist

$$\binom{4p-2}{p} = \frac{(4p-2)\cdot\ldots\cdot(3p+1)\cdot 3p\cdot(3p-1)}{1\cdot 2\cdot\ldots\cdot(p-1)\cdot p},$$

also $$(p-1)!\binom{4p-2}{p} \equiv 3\cdot(p-1)! \pmod{p},$$

d.h. $$\binom{4p-2}{p} \equiv 3 \pmod{p}.$$

Analog $$\binom{3p-2}{p} \equiv 2 \pmod{p} \text{ und } \binom{2p-2}{p} \equiv 1 \pmod{p}.$$

Somit

$$3 - 2(p,y) + (2p,y) \equiv 0 \pmod{p} \quad \ldots\ldots (2)$$

Aus (1) − (2) folgt die Behauptung.

**Folgerung 9.21** Für alle $X \subseteq \mathbb{Z}^2$ mit $|X| = 4p-3$ mit $(p, X) = 0$ ist

$$2 - (p-1, X) + (3p-1, X) \equiv 0 \pmod{p}.$$

**Beweis.** OBdA $(0,0) \notin X$. Lemma 9.20 angewandt auf $Y = X \cup \{(0,0)\}$ liefert

$$2 - (p-1, X) - (p, X) + (3p-1, X) + (3p, X) \equiv 0 \pmod{p}.$$

Da $(p, X) = 0$ vorausgesetzt ist, genügt es $(3p, X) = 0$ zu beweisen.

Das macht man mit einem Trick von Alon & Dubiner:

Angenommen $(3p, X) > 0$. Wähle $Z \subseteq X$ mit $|Z| = 3p$ und $\sum Z \equiv (0,0) \pmod{p}$

Betrachte $Z' \subseteq Z$ mit $|Z'| = 3p-1$. Nach Lemma 9.19 ist

$1 - (p, Z') + (2p, Z') \equiv 0 \pmod{p}$. Wegen $Z' \subseteq X$ und $(p, X) = 0$ ist $(p, Z') = 0$. Nun $(2p, Z') \neq 0$. Wähle $Q \subseteq Z'$ mit $|Q| = 2p$ und $\sum Q \equiv (0,0)$. Nun $|Z \setminus Q| = p$, $\sum (Z \setminus Q) \equiv (0,0) \pmod{p}$ Wid.

## Beweis der Kemnitz-Vermutung.

Angenommen, es gäbe eine Primzahl $p$ und $X \subseteq \mathbb{Z}^2$ mit $|X| = 4p-3$ und $(p, X) = 0$. Wir wissen $p \neq 2$. Aus Folgerung 9.21 ergibt sich

$$(p-1, X) \not\equiv (3p-1, X) \pmod{p}$$

Es sei $\Omega$ die Anzahl der Partitionen $X = A \dot\cup B \dot\cup C$ mit

$$|A| = p-1, \quad |B| = p-2, \quad |C| = 2p$$

$$\sum A \equiv \sum C \equiv (0,0) \pmod{p}, \quad \sum B \equiv \sum X \pmod{p}.$$

Für alle $A \subseteq X$ mit $|A| = p-1$, $\sum A \equiv (0,0) \pmod{p}$ ist

$$|X \setminus A| = 3p-2, \text{ also } 1 - \underbrace{(p, X \setminus A)}_{=0} + (2p, X \setminus A) \equiv 0 \pmod{p},$$

d.h. $(2p, X \setminus A) \equiv -1 \pmod{p}$.

Dies zeigt $\Omega \equiv \sum_A (2p, X \setminus A) \equiv \sum_A (-1) \equiv -(p-1, X) \pmod{p}$.

Analog gilt $(z_p, X \setminus B) \equiv -1 \pmod{p}$ für alle $B \subseteq X$ mit $|B| = p-2$.

Also

$$\Omega \equiv \sum_B (z_p, X \setminus B) \equiv \sum_{X \setminus B} (-1) \equiv -(3_p - 1, X) \pmod{p}.$$

Insgesamt

$$(p-1, X) \equiv -\Omega \equiv (3_p - 1, X) \pmod{p}.$$ Wid. □

# Zukunft.

**Satz (Hilbert)** $\forall k \; \exists g(k) \quad N_0 = g(k) \, N_0^k$

**Satz (Weyl)** $\alpha$ irrational $\Rightarrow$

$(\alpha n^k)_{n \in \mathbb{N}}$ gleichverteilt mod. 1

"**Satz**" Oft gilt

$$\left| \sum_{n=1}^{N} e^{2\pi i \alpha n^2} \right| \leq O(N^{314})$$

**Satz** $A \subseteq \mathbb{F}_3^n$ enthält keine $AP_3$

$\Rightarrow |A| \leq 2.99^n$

**Satz (Roth)** $A \subseteq [N]$ $AP_3$-frei

$$\Rightarrow |A| \leq \frac{CN}{\log\log N}$$

**Satz (Bourgain)** Es gilt sogar

$$|A| \leq \frac{CN}{\sqrt{\log N}}$$

. . . .

**Satz (Gowers)** $A \subseteq [N]$ $AP_4$-frei $\Rightarrow$ $|A| \leq \frac{CN}{(\log\log\log N)^c}$.