Alexandra Merz, Christian Semrau **WS 2002/03**
(Aus Kapitel 3 eines Skripts „Einführung in die Zahlentheorie“ von Alexander Schmidt.)

Der Satz von Chevalley-Warning

Seien $f_i \in \mathbb{F}_p[X_1, \dots, X_r], f_i \neq 0$ für $i = 1, \dots, n$. Bezeichne (S) das Gleichungssystem

$$f_i(x_1, \dots, x_r) = 0,\ i = 1, \dots, n.$$

Die Lösungsmenge $L(S)$ dieses Systems ist eine Teilmenge von $(\mathbb{F}_p)^r$. Trivialerweise ist damit $0 \leq |L(S)| \leq p^r$. Für ein *Monom* $X_1^{\mu_1} \cdots X_r^{\mu_r}$ heißt $\mu = \mu_1 + \cdots + \mu_r$ der *Grad* des Monoms. Der *Grad eines Polynoms* f ist das Maximum der Grade der in f auftretenden Monome, geschrieben als $\deg f$. f heißt *homogen*, wenn alle Monome in f den gleichen Grad haben.

Theorem (Chevalley-Warning). *Ist* $\sum_{i=1}^n \deg f_i < r$*, so gilt*

$$|L(S)| \equiv 0 \mod p.$$

Zunächst betrachten wir für jedes $u \in \mathbb{N}$ das Monom X^u in einer Variablen vom Grad u. Wir setzen $X^0 = 1$.

Lemma. $\sum_{x \in \mathbb{F}_p} x^u = \begin{cases} 0 & , u = 0, \\ 0 & , u \geq 1 \textit{ und } (p-1) \nmid u, \\ -1 & , u \geq 1 \textit{ und } (p-1) \mid u. \end{cases}$

Beweis. Für $u = 0$ gilt offensichtlich $\sum_{x \in \mathbb{F}_p} x^u = p \cdot 1 = 0$. Ist $u = (p-1)v$ mit $v \geq 1$, so ist

$$\sum_{x \in \mathbb{F}_p} x^u = \sum_{x \in \mathbb{F}_p} (x^{p-1})^v.$$

Auf der rechten Seite sind $p-1$ Summanden gleich 1 und einer 0. Also ist die Summe gleich $p - 1 = -1$. Ist nun $u \geq 1$ nicht durch $p-1$ teilbar, so gibt es ein $x_0 \in \mathbb{F}_p$ mit $x_0^u \neq 1$. Multiplizieren wir $\sum_{x \in \mathbb{F}_p} x^u$ mit x_0^u, so permutieren sich nur die Summanden und wir erhalten

$$x_0^u \left(\sum_{x \in \mathbb{F}_p} x^u \right) = \left(\sum_{x \in \mathbb{F}_p} (x_0 x)^u \right) = \sum_{x \in \mathbb{F}_p} x^u$$

und damit $(x_0^u - 1)(\sum_{x \in \mathbb{F}_p} x^u) = 0$. Wegen $x_0^u \neq 1$ folgt hieraus, dass die Summe gleich 0 ist. □

Beweis des Theorems von Chevalley-Warning. Wir setzen $P := \prod_{i=1}^n (1 - f_i^{p-1}) \in F_p[X_1, \dots, X_r]$.
Ist $x = (x_1, \dots, x_r)$ eine simultane Nullstelle, so gilt $P(x) = 1$. Ist $f_i(x) \neq 0$ für ein i, so ist $f_i(x)^{p-1} = 1$, also $1 - f_i(x)^{p-1} = 0$ und folglich auch $P(x) = 0$. Damit ist P die charakteristische Funktion von $L(S)$. Daher gilt

$$|L(S)| \equiv \sum_{x \in (\mathbb{F}_p)^r} P(x) \mod p.$$

Es bleibt also zu zeigen, dass $\sum_{x \in (\mathbb{F}_p)^r} P(x) = 0$ gilt. Es ist $\deg(1 - f_i^{p-1}) \leq (p-1)(\deg f_i)$. P ist ein Polynom mit $\deg P = \sum_{i=1}^n \deg(1 - f_i^{p-1}) \leq \sum_{i=1}^n (p-1)(\deg f_i) < (p-1)r$ nach Voraussetzung. Wir können daher P als Linearkombination von Monomen der Form $X_1^{\mu_1} \cdots X_r^{\mu_r}$ mit $\mu_1 + \cdots + \mu_r < (p-1)r$ schreiben. Es ist in jedem dieser Monome mindestens ein $\mu_i < (p-1)$. Nun gilt nach dem allgemeinen Distributivgesetz

$$\sum_{x \in (\mathbb{F}_p)^r} x_1^{\mu_1} \cdots x_r^{\mu_r} = \left(\sum_{x_1 \in \mathbb{F}_p} x_1^{\mu_1} \right) \cdots \left(\sum_{x_r \in \mathbb{F}_p} x_r^{\mu_r} \right).$$

Nach obigen Lemma ist mindestens einer der Faktoren gleich 0, also auch das Produkt.
Daher ist $\sum_{x \in (\mathbb{F}_p)^r} P(x)$ gleich der Summe von Nullen und also selbst gleich 0. □

Bemerkung. *Für jeden endlichen Körper K der Charakteristik p ist die Anzahl der Lösungen eines Gleichungssystem aus Polynomen $f_i \in K[X_1, \dots, X_r]$ durch p teilbar, wenn $\sum \deg f_i < r$.*

Korollar. *Sei $f \in \mathbb{F}_p[X_1, \dots, X_r]$ homogen mit $0 < \deg f < r$. Dann hat f eine nichttriviale Nullstelle.*

Beweis. Der Punkt $(0, \dots, 0) \in (\mathbb{F}_p)^r$ ist Nullstelle von f, weil f kein Absolutglied hat. Da $\deg f < r$, hat f nach dem Theorem mindestens $p \geq 2$ Nullstellen, also auch eine nichttriviale. □

Korollar. *Das Polynom $f = aX^2 + bY^2 + cZ^2 \in \mathbb{F}_p[X, Y, Z]$ hat eine nichttriviale Nullstelle.*