Karlsruher Institut für Technologie

Seminarvortrag
Ein Satz von Gauß

von

Johannes Lorenz

Seminar
Elliptische Kurven

Betreuer: Prof. Dr. Claus-Günther Schmidt
Betreuende Mitarbeiterin: Dipl.-Math Jingwei Zhao

Inhaltsverzeichnis

Kapitel 1

Ein Satz von Gauß

1.1 Einführung

Sei $n \in \mathbb{N}$ fest. Die Fermat-Kurve ist durch die Gleichung

$$x^n + y^n = 1$$

gegeben. Nach dem großen fermatschen Satz gibt es für diese Gleichung in $\mathbb{Q}$ nur triviale Lösungen [Wik11b].

Im Folgenden sei $p \in \mathbb{N}$ prim und fest; und unser Körper sei der $\mathbb{F}_p$. Wir interessieren uns hier für die Anzahl Lösungen für $n = 3$ im projektiven Raum. Das heißt, wir suchen Lösungen der Gleichung

$$x^3 + y^3 + z^3 = 0,$$

wobei $(x, y, z) \neq (0, 0, 0)$ und $(x, y, z) = (\lambda x, \lambda y, \lambda z)$ für alle $\lambda \in \mathbb{F}_p^\times$.

1.2 Satz von Gauß

Satz 1.2.1 (Gauß)**.** *Sei p eine feste Primzahl. Sei M_p die Anzahl projektiver Lösungen der Gleichung*

$$x^3 + y^3 + z^3 = 0$$

mit $x, y, z \in \mathbb{F}_p^3$. Dann gilt:

1. *Falls $p \not\equiv 1 \mod 3$, dann ist $M_p = p + 1$.*
2. *Falls $p \equiv 1 \mod 3$, dann gilt:*

$$\exists A, B \in \mathbb{Z} : 4p = A^2 + 27B^2.$$

A und B sind bis auf Vorzeichen eindeutig, und wenn wir das Vorzeichen von A fest wählen, so dass $A \equiv 1 \mod 3$, so gilt:

$$M_p = p + 1 + A.$$

Zusatz: Falls $p \equiv 1 \mod 3$*, so gilt:*

$$9 | M_p.$$

Beweis. Sei $\varphi : \mathbb{F}_p^\times \to \mathbb{F}_p^\times : a \mapsto a^3$.

Lemma 1. *Es gilt:*

$$p \equiv 1 \mod 3 \Leftrightarrow \ker \varphi \gneq \{1\}.$$

Beweis.

$$\begin{aligned}
&3 \mid p-1 \\
&\Leftrightarrow \exists n \in \mathbb{N} : 0 < n < p-1,\ 3n \in (p-1)\mathbb{Z} \\
&\Leftrightarrow \exists n \in \mathbb{N} : 0 < n < p-1,\ \varphi(z^n) = z^{3n} = z^{p-1} = 1 \text{ für } \langle z \rangle = \mathbb{F}_p^\times \\
&\Leftrightarrow \ker \varphi \gneq \{1\}
\end{aligned}$$

□

Lemma 2. *Sei* $p \in \mathbb{N}$ *prim. Es gilt:*

$$|\{(x,y,z) \in \mathbb{P}^2(\mathbb{F}_p) | x+y+z = 0\}| = p+1.$$

Beweis. Sei k ein beliebiger Körper, $f(X,Y,Z) := X+Y+Z$. Betrachte $V := V_{\text{aff}}(f)$ in $\mathbb{A}^3(k)$. Offensichtlich ist V_{aff} ein Untervektorraum von $\mathbb{A}^2(k)$. Es ist $dim(V_{\text{aff}}) \leq 2$, denn $Z = X - Y$. Aber die Vektoren $e_1 - e_3$ und $e_2 - e_3$ liegen in V_{aff} und sind linear unabhängig, also $dim(V_{\text{aff}}) \geq 2$. Also $dim(V_{\text{aff}}) = 2$. Also gibt es einen bijektiven Morphismus, so dass gilt:

$$\mathbb{P}^1(k) = \mathbb{A}^2(k) - 0/\sim \cong V_{\text{aff}}(f) - 0/\sim = V_{\text{proj}}(f).$$

Man nennt $\mathbb{P}^1(k)$ auch projektive Gerade.

Nun gilt:

$$|\mathbb{P}^1(\mathbb{F}_p)| = |\mathbb{A}^2(\mathbb{F}_p) \setminus \{0\}|/(p-1) = (p^2-1)/(p-1) = p+1,$$

denn jede Gerade beinhaltet wegen der Charakteristik genau p Punkte, von denen einer der Nullpunkt ist. Ein Beispiel für $p = 5$ ist in Abbildung 1.1 zu sehen. Damit folgt die Behauptung:

$$|\{(x,y,z) \in \mathbb{P}^2(\mathbb{F}_p) | x+y+z = 0\}| = |\mathbb{P}^1(\mathbb{F}_p)| = p+1.$$

Details zu den Begriffen in [Alg09]. □

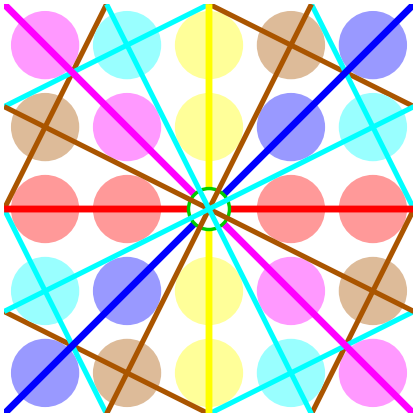

Abbildung 1.1: Beispiel für die Konstruktion des $\mathbb{P}^1(\mathbb{F}_5)$. Quelle: [Wik11a].

Für den ersten Fall sei $p \not\equiv 1 \mod 3$. Lemma 1 und 2 besagen:

$$\begin{aligned} &3 \nmid p-1 \Leftrightarrow \ker\varphi = 1 \Leftrightarrow \varphi \in Aut(\mathbb{F}_p^\times) \\ &\Rightarrow M_p = |\{(x,y,z) \in \mathbb{P}^2(\mathbb{F}_p) | (x^3+y^3+z^3=0)\}| \\ &= |\{(x,y,z) \in \mathbb{P}^2(\mathbb{F}_p) | (x+y+z=0)\}| = p+1. \end{aligned}$$

Betrachte im Folgenden nur den zweiten Fall; es sei also $p =: 3m+1, m \in \mathbb{N}$. Definiere $R := \operatorname{im}\varphi \cong \mathbb{F}_p^\times / \ker\varphi$. Als zyklische Untergruppe ist $\ker\varphi =: \langle u \rangle = \{u, u^2, u^3 = 1\}$ und $u \neq 1$, da nach Lemma 1 $\ker\varphi \gneq 1$. Also $(\mathbb{F}_p^\times : R) = 3$. Es gibt 3 Nebenklassen, hier R, S, T. Man nennt sie auch kubische Reste. Vorsicht: Die Linkstranslation ist zwar bijektiv, aber nicht homomorph. S und T sind i.A. keine Untergruppen von $\mathbb{F}_p^\times$.

Beachte:

- $\mathbb{F}_p = \{0\} \cup R \cup S \cup T$.
- Sei $s \notin R$, dann induzieren (O.E.) $sR =: S$ und $s^2R = sS = T$.
- Es ist $-1 = -1^3 \in R$, also $-R = R, -S = -(RS) = RS = S, -T = T$.

Seien $X, Y, Z \subseteq \mathbb{F}_p$. Definiere:

$$[XYZ] := [X,Y,Z] := |\{(x,y,z) \in (X,Y,Z) : x+y+z=0\}|.$$

Lemma 3. *Es gilt:*

$$M_p = 9(\frac{[RRR]}{m} + 1).$$

Beweis. Seien also $x^3+y^3+z^3 = 0, (x,y,z) \in \mathbb{F}_p^3$.

Fall 1.2.1.1. Seien $x, y, z \neq 0$. Dann ist

$$\begin{aligned} &|\{(x,y,z) \in \mathbb{F}_p^3 : x^3 + y^3 + z^3 = 0\}| \\ = 3^3 &|\{(r_1, r_2, r_3) \in R^3 : r_1 + r_2 + r_3 = 0\}| \\ &= 27[RRR]. \end{aligned}$$

Das gibt $\frac{27[RRR]}{p-1} = \frac{9[RRR]}{m}$ projektive Lösungen.
Fall 1.2.1.2. Sei zunächst $z = 0$. Wegen Projektivität ist $x \neq 0$ und $y \neq 0$. Für festes x ist

$$|\{y \in \mathbb{F}_p : x^3 = -y^3\}| = |-x, -ux, -u^2x| = 3,$$

für bel. $u \in \mathbb{F}_p^\times, ord(u) = 3$. Also $|\{(x,y) \in \mathbb{F}_p^2 : x^3 + y^3 = 0\}| = 3(p-1)$. Analog für $x \neq 0$ und $y \neq 0$, also

$$\{(x,y,z) \in \mathbb{F}_p^2 : x^3 + y^3 + z^3 = 0\}| = 9(p-1).$$

Also 9 projektive Lösungen.

Insgesamt gilt:

$$M_p = \frac{9[RRR]}{m} + 9 = 9(\frac{[RRR]}{m} + 1).$$

□

Lemma 4. *Seien $X_1, X_2, X_3, X_4 \subseteq \mathbb{F}_p$. Dann gelten:*

1. $[X_1X_2(X_3 \cup X_4)] = [X_1X_2X_3] + [X_1X_2X_4]$ *falls* $X_3 \cup X_4 = \emptyset$.
2. $[X_1X_2X_3] = [aX_1, aX_2, aX_3]$ *falls* $a \neq 0$.
3. $\forall \sigma \in S_3 : [X_1X_2X_3] = [X_{\sigma(1)}X_{\sigma(2)}X_{\sigma(3)}]$.

Beweis. Punkte 1 und 3 sind klar. Punkt 2 gilt wegen $|aX_i| = |X_i|, i \in \{1,2,3\}$. □

Lemma 5. *Es gilt:*

$$M_p = 9\frac{[RTS]}{m}.$$

Beweis.

$$m^2 = [RR\mathbb{F}_p] = \underbrace{[RR\{0\}]}_{=m} + [RRR] + \underbrace{[RRS]}_{=[sRsRsS]=[SST](s\in S)} + \underbrace{[RRT]}_{=[tRtRtT]=[TTS](t\in T)} \tag{5.1}$$

$$m^2 = [\mathbb{F}_pTS] = \underbrace{[\{0\}TS]}_{=0, \text{ da } -S\cap T=S\cap T=\emptyset} + [RTS] + [STS] + [TTS] \tag{5.2}$$

Berechne (5.1) − (5.2), so folgt:

$$0 = m + [RRR] - [RTS] \Leftrightarrow [RRR] = [RTS] - m$$
$$\Leftrightarrow M_p = 9(\frac{\overbrace{[RTS] - m}^{[RRR]}}{m} + 1) = 9\frac{[RTS]}{m}.$$

□

Es seien ab jetzt $a := [STR]/m$, $b := [STS]/m$, $c := [STT]/m \in \mathbb{Q}$. Damit gilt:

$$(a + b + c) = \frac{[STR] + [STS] + [STT]}{m} = \frac{[ST\mathbb{F}_p] - [ST0]}{m} = m.$$

Sei $\zeta \in \mathbb{C}$ im ganzen Dokument eine p-te primitive Einheitswurzel . Definiere kubische Gauß-Summen:

$$\alpha_{1+3\mathbb{Z}} := \sum_{r\in R} \zeta^r, \alpha_{2+3\mathbb{Z}} := \sum_{s\in S} \zeta^s, \alpha_{3+3\mathbb{Z}} := \sum_{t\in T} \zeta^t.$$

Lemma 6. *Es sind $a, b, c \in \mathbb{Z}$, und es gilt:*

$$\forall i \in \mathbb{Z}/3\mathbb{Z} : \alpha_{i+1}\alpha_{i+2} = a\alpha_i + b\alpha_{i+1} + c\alpha_{i+2}.$$

Beweis. Wir zeigen das für $i = 1$. Der Rest folgt analog. Definiere $N_x := |\{(s, t) \in (S, T) : s + t = x\}|$.

$$r \in R \Rightarrow N_x = [ST{-}x] = [rS, rT, -rx] = [S, T, -rx] = N_{rx}.$$

Wir sehen:

$$mN_x = [S, T, Rx] = \begin{cases} [STR] = ma \text{ falls } x \in R, \\ [STS] = mb \text{ falls } x \in S, \\ [STT] = mc \text{ falls } x \in T. \end{cases}$$

Klar sind $a, b, c \in \mathbb{Z}$. Es gilt:

$$\alpha_2\alpha_3 = \sum_{s\in S}\sum_{t\in T} \zeta^s\zeta^t = \sum_{s\in S, t\in T} \zeta^{s+t} = \sum_{x\in\mathbb{F}_p} N_x\zeta^x = a\alpha_1 + b\alpha_2 + c\alpha_3.$$

□

Aus dem Lemma folgt $M_p = 9a \in 9\mathbb{Z}$, und damit unmittelbar der Zusatz.
Setze $k := 2a - b - c = 3a - m$.

Lemma 7. *Es gelten folgende Gleichungen.*

$$\sum_{i\in\mathbb{F}_3} \alpha_i = -1 \tag{7.1}$$

$$\sum_{i\in\mathbb{F}_3} \alpha_i\alpha_{i+1} = -m \tag{7.2}$$

$$\sum_{i\in\mathbb{F}_3} \alpha_i^2 = 1 + 2m \tag{7.3}$$

$$\prod_{i\in\mathbb{F}_3} \alpha_i = \frac{a+km}{3} \tag{7.4}$$

Beweis.

$$0 = \zeta^p - 1 = (\zeta - 1)(\sum_{i=0}^{p-1} \zeta^i) \overset{\zeta\neq 1}{\Leftrightarrow} 0 = \sum_{i=0}^{p-1} \zeta^i$$

$$\Rightarrow \alpha_1 + \alpha_2 + \alpha_3 = (\sum_{i=0}^{p-1} \zeta^i) - \zeta^0 = -1 \Rightarrow (7.1)$$

$$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = (a+b+c)(\alpha_1+\alpha_2+\alpha_3) = -m \Rightarrow (7.2)$$

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = (\alpha_1+\alpha_2+\alpha_3)^2 - 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = 1 + 2m \Rightarrow (7.3)$$

$$\begin{aligned} 3\alpha_1\alpha_2\alpha_3 &= \sum_{i\in\mathbb{Z}/3\mathbb{Z}} \alpha_i(\alpha_{i+1}\alpha_{i+2}) \\ &= \sum_{i\in\mathbb{Z}/3\mathbb{Z}} \alpha_i(a\alpha_i + b\alpha_{i+1} + c\alpha_{i+2}) \\ &= a(\alpha_1^2+\alpha_2^2+\alpha_3^2) + (b+c)(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3) \\ &= a(1+2m) + (b+c)(-m) = a + m(2a-b-c) = a + km \Rightarrow (7.4) \end{aligned}$$

□

Lemma 8. *Sei*

$$F(t) := \prod_{i\in\mathbb{F}_3}(t-\alpha_i) = t^3 + t^2 - mt - (a+km)/3 \in \mathbb{Q}[X].$$

Dann ist

$$\sqrt{D_F} = (b-c)p.$$

Beweis.

$$\begin{aligned}\sqrt{D_F} &= \prod_{i\in\mathbb{F}_3}(\alpha_i - \alpha_{i+1}) \\ &= \sum_{i\in\mathbb{F}_3}(\alpha_{i+1}\alpha_{i+2}(\alpha_{i+1} - \alpha_{i+2})) \\ &= \sum_{i\in\mathbb{F}_3}((a\alpha_i + b\alpha_{i+1} + c\alpha_{i+2})(\alpha_{i+1} - \alpha_{i+2})) \\ &= (b-c)(\alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_1\alpha_2 - \alpha_1\alpha_3 - \alpha_2\alpha_3) \\ &= (b-c)((1+2m) - (-m)) = (b-c)p,\end{aligned}$$

wobei die vierte aus der dritten Zeile folgt, indem sich die a gegenseitig aufheben. □

Lemma 9. *Das Polynom $G(t) = t^3 - 3pt - (3k-2)p$ hat die Diskriminante*

$$D_G = 27^2 D_F.$$

Beweis. Definiere analog zu den α_i entsprechende $\beta_{i+3\mathbb{Z}} := 1 + 3\alpha_i$, wobei $1 \leq i \leq 3$. Behauptung:

$$\prod_{i\in\mathbb{F}_3}(t - \beta_i) = t^3 - 3pt - (3k-2)p = G(t).$$

Offensichtlich ist dann

$$\sqrt{D_G} = \prod_{i\in\mathbb{F}_3}(\beta_i - \beta_{i+1}) = \prod_{i\in\mathbb{F}_3} 3(\alpha_i - \alpha_{i+1}) = 27\sqrt{D_F}.$$

Zu zeigen sind also die folgenden Gleichungen.

$$\sum_{i\in\mathbb{F}_3}\beta_i = 0 \tag{9.1}$$

$$\sum_{i\in\mathbb{F}_3}\beta_i\beta_{i+1} = -3p \tag{9.2}$$

$$\prod_{i\in\mathbb{F}_3}\beta_i = (3k-2)p \tag{9.3}$$

$$\sum_{i\in\mathbb{F}_3}\beta_i = 3 + 3\sum_{i\in\mathbb{F}_3}\alpha_i = 3 + 3(-1) = 0$$

$$\begin{aligned}\sum_{i\in\mathbb{F}_3}\beta_i\beta_{i+1} &= \sum_{i\in\mathbb{F}_3}((3\alpha_i + 1)(3\alpha_{i+1} + 1)) \\ &= 9\sum_{i\in\mathbb{F}_3}\alpha_i\alpha_{i+1} + 3\sum_{i\in\mathbb{F}_3}(\alpha_i + \alpha_{i+1}) + 3\sum_{i\in\mathbb{F}_3}1 \\ &= -9m + 3(-1-1) + 3 = 9m - 3 = -3p\end{aligned}$$

$$\begin{aligned}\prod_{i\in\mathbb{F}_3}\beta_i &= \prod_{i\in\mathbb{F}_3} 1+3\alpha_i \\ &= 27\prod_{i\in\mathbb{F}_3}\alpha_i + 9\sum_{i\in\mathbb{F}_3}\alpha_i\alpha_{i+1} + 3\sum_{i\in\mathbb{F}_3}\alpha_i + 1 \\ &= 9(a+km) + 9(-m) + 3(-1) + 1 \\ &= 3(k+m) + 3k3m - 3(3m) - 2 \\ &= 3k + (p-1) + 3k(p-1) - 3(p-1) - 2 = \\ &= (p-1)(3k-2) + 3k - 2 = (3k-2)p\end{aligned}$$

□

Die Diskriminante von D_G kann man aber auch mit der allgemeinen Diskriminanten-Formel für kubische Polynome ohne quadratischen Term ausrechnen. Diese besagt:

Satz 1.2.2. *Ein Polynom der Form x^3+px+q hat die Determinante $\Delta = -4p^3-27q$.*

Beweis. Siehe [Wik10]. □

Hier also:

$$D_G = -4(-3p)^3 - 27((3k-2)p)^2 = 4\cdot 27p^3 - 27(3k-2)^2p^2.$$

Ein Vergleich ergibt:

$$\begin{aligned}4\cdot 27p^3 - 27(3k-2)^2p^2 = D_G = (27)^2D_F = (27)^2(b-c)^2p^2 \\ \Leftrightarrow 4p = (3k-2)^2 + 27(b-c)^2.\end{aligned}$$

Aus $A := 3k-2, B := (b-c)$ folgt schließlich:

$$M_p = 9a = 3(k+m) = 3k+p-1 = p+1-A \text{ sowie } 4p = A^2+27B^2.$$

Lemma 10. *Angenommen, für $A, B, \tilde{A}, \tilde{B}$ gelte:*

$$4p = A^2 + 27B^2, \tag{10.1}$$

$$4p = \tilde{A}^2 + 27\tilde{B}^2 \text{ und} \tag{10.2}$$

$$A, \tilde{A} \equiv 1(3). \tag{10.3}$$

Dann folgt:

$$A = \tilde{A}, B = \tilde{B}.$$

Beweis. Berechne $((\tilde{B}^2\cdot(10.2)) - (B^2\cdot(10.1)))$:

$$\begin{aligned}4p(\tilde{B}^2 - B^2) = (A^2+27B^2)\tilde{B}^2 - (\tilde{A}^2+27\tilde{B}^2)B^2 = (A\tilde{B}+\tilde{A}B)(A\tilde{B}-\tilde{A}B) \\ \overset{\text{O.E.}}{\Rightarrow} p|(A\tilde{B}-\tilde{A}B).\end{aligned}$$

Anderseits kann man (10.2) mit (10.1) multiplizieren:

$$\begin{aligned} 16p^2 &= A^2\tilde{A}^2 + 27B^2\tilde{A}^2 + 27\tilde{B}^2A^2 + (27)^2B^2\tilde{B}^2 \\ \Rightarrow 16p^2 - (A\tilde{A} + 27B\tilde{B})^2 &= 27(A\tilde{B} - \tilde{A}B)^2, \end{aligned}$$

wobei sich die $2ab$-Summanden aufheben. Alle Terme sind also Vielfache von p:

$$\begin{aligned} 16 > 16 - (\frac{A\tilde{A} + 27B\tilde{B}}{p})^2 &= 27(\frac{A\tilde{B} - \tilde{A}B}{p})^2 \\ \Rightarrow A\tilde{B} - \tilde{A}B = 0 \Leftrightarrow \frac{\tilde{B}}{B} &= \frac{\tilde{A}}{A}. \end{aligned}$$

Einsetzen ergibt schlussendlich:

$$\begin{aligned} A^2 + 27B^2 = 4p = \tilde{A}^2 + 27\tilde{B}^2 = \frac{\tilde{B}}{B}A^2 + 27\frac{\tilde{A}}{A}B^2 &= \frac{\tilde{A}}{A}(A^2 + 27B^2) \\ \Rightarrow \frac{\tilde{A}}{A} \in \{-1, +1\} \overset{(10.3)}{\Leftrightarrow} \tilde{A} &= A. \end{aligned}$$

□

Damit ist der Satz bewiesen. □

1.3 Beispiele

Für den Fall $p \not\equiv 1 (\text{mod } 3)$ ist die Berechnung von $M_p = p+1$ trivial. Falls $p \equiv 1 (\text{mod } 3)$, so hilft es, dass (wegen dem Zusatz) $A \equiv -p - 1 \mod 9$ ist. Für B kann man die Gleichung $4p = A^2 + 27B^2$ als Kongruenz bezüglich kleiner Primzahlen betrachten, was den Suchraum erheblich einschränkt.

Folgende Tabelle enthält ein paar Zahlenbeispiele für den zweiten Fall.

p	A	B	$M_p = A + p + 1$
7	1	1	9
13	-5	1	9
19	7	1	27
31	4	2	36
4027	-104	14	3924

Literaturverzeichnis

[Alg09] *Algebraische Geometrie - Wintersemester 2008/2009.* http://mitschriebwiki.nomeata.de/AlgGeo.html, 2009. Seite besucht am 20.12.2011.

[Wik10] *Projective line over a finite field.* http://commons.wikimedia.org/wiki/Projective_line_over_a_finite_field, 2010. Seite besucht am 20.12.2011.

[Wik11a] *Discriminant - Formula.* http://en.wikipedia.org/wiki/Discriminant#Formula_2, 2011. Seite besucht am 20.12.2011.

[Wik11b] *Großer fermatscher Satz.* http://de.wikipedia.org/wiki/Gro%C3%9Fer_fermatscher_Satz, 2011. Seite besucht am 20.12.2011.