Vortrag zum Seminar Zahlentheorie bei Herrn Bogopolski

Katrin Trosky

15. Mai 2017

In den folgenden Seiten werden die ersten beiden Paragraphen des Kapitel 8, des Buches „A Classical Introduction to Modern Number Theory“ (second edition, Springer 1990) von Kenneth Ireland und Michael Rosen behandelt.

Kapitel 8. Gauß- und Jacobi-Summe

In Kapitel 6 haben wir den Begriff der quadratischen Gauß-Summe eingeführt. In diesem Kapitel wird ein allgemeinerer Begriff der Gauß-Summe eingeführt. Diese Summen haben mehrere Verwendungen. Hier werden wir das Problem der Zählung der Lösungsanzahl von Gleichungen in einem Endlichen Körper betrachten. Um die Dinge so einfach wie möglich zu halten, beschränken wir uns auf den endlichen Körper $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

1 Multiplikative Charaktere

Definition 8.1.1:

Ein *multiplikativer Charakter* von $\mathbb{F}_p$ ist eine Abbildung $\chi : \mathbb{F}_p^* \longrightarrow \mathbb{C}\backslash\{0\}$, die folgendes erfüllt:

$$\chi(ab) = \chi(a)\chi(b) \quad \forall\, a, b \in \mathbb{F}_p^*$$

Beispiele für multiplikative Charaktere sind das Legendre Symbol $(\frac{a}{p})$, wenn es als eine Funktion der Nebenklassen von a modulo p betrachtet wird, oder aber auch der triviale multiplikative Charakter, der durch die Zuordnung $\varepsilon(a) = 1$ für alle $a \in \mathbb{F}_p^*$ definiert wird. Oftmals ist es sinnvoll den Definitionsbereich der multiplikativen Charaktere auf ganz $\mathbb{F}_p$ zu erweitern. Falls

$\chi \neq \varepsilon$ ist, so definieren wir $\chi(0) = 0$ und $\varepsilon(0) = 1$. Die Nützlichkeit dieser Definition wird später ersichtlich.

Satz 8.1.2:

Sei χ ein multiplikativer Charakter und $a \in \mathbb{F}_p^*$. Dann gelten:

(*a*) $\chi(1) = 1$,

(*b*) $\chi(a)$ ist die $(p-1)te$ Einheitswurzel,

(*c*) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Bemerkung:

In Teil (*a*) ist die 1 auf der linken Seite die Einheit von $\mathbb{F}_p$, die 1 auf der rechten Seite die komplexe Zahl 1. Der Balken in (*c*) meint die komplexe Konjugation.

Beweis:

(*a*) Es ist $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$. Daher ist $\chi(1) = 1$, da $\chi(1) \neq 0$.

(*b*) Um (*b*) zu überprüfen beachte, dass $a^{p-1} = 1$, $1 = \chi(1) = \chi(a^{p-1}) = \chi(a)^{p-1}$ impliziert.

(*c*) Um (*c*) zu überprüfen, beachte, dass $1 = \chi(1) = \chi(a^{-1}a) = \chi(a^{-1})\chi(a)$. Dies zeigt, dass $\chi(a^{-1}) = \chi(a)^{-1}$. Nach Teil (*b*) ist $\chi(a)$ eine komplexe Zahl mit Absolutbetrag 1. Somit gilt $\chi(a)^{-1} = \overline{\chi(a)}$.

□

Satz 8.1.3:

Sei χ ein multiplikativer Charakter. Dann gilt:

$$\sum_{t=0}^{p-1} \chi(t) = \chi(0) + \chi(1) + ... + \chi(p-1) = \begin{cases} 0, & \chi \neq \varepsilon \\ p, & \chi = \varepsilon \end{cases}$$

Beweis:

Für den Fall $\chi = \varepsilon$ ist die letzte Behauptung offensichtlich, denn

$$\chi(t) = \varepsilon(t) = 1 \;\Rightarrow\; \sum_{t=0}^{p-1} \chi(t) = \sum_{t=0}^{p-1} 1 = p.$$

Sei nun $\chi \neq \varepsilon$. Dann gibt es ein $a \in \mathbb{F}_p^*$, sodass $\chi(a) \neq 1$. Sei $T = \sum_{t=0}^{p-1} \chi(t)$. Dann gilt

$$\chi(a)T = \chi(a) \sum_{t=0}^{p-1} \chi(t) = \sum_{t=0}^{p-1} \chi(a)\chi(t) = \sum_{t=0}^{p-1} \chi(at) = T$$

Die letzte Gleichheit folgt, da at alle Elemente von $\mathbb{F}_p$ durchläuft, sofern t alle Elemente von $\mathbb{F}_p$ durchläuft. Da $\chi(a)T = T$ und $\chi(a) \neq 1$ gelten, folgt $T = 0$. □

Definition 8.1.4:

Die multiplikativen Charaktere bilden eine Gruppe, wenn man folgende Definitionen benutzt:

(1) Falls χ und λ Charaktere sind, dann ist $\chi\lambda$ die Abbildung, die $a \in \mathbb{F}_p^*$ nach $\chi(a)\lambda(a)$ abbildet.

(2) Falls χ ein Charakter ist, dann ist χ^{-1} die Abbildung, die $a \in \mathbb{F}_p^*$ nach $\chi(a)^{-1}$ abbildet.

Dass es sich bei diesen Abbildungen wieder um Charaktere handelt, überprüft man schnell. Die Identität dieser Gruppe ist offensichtlich der triviale Charakter ε.

Satz 8.1.5:

Die Gruppe der Charaktere ist eine zyklische Gruppe der Ordnung $(p-1)$. Falls $a \in \mathbb{F}_p^*$ und $a \neq 1$ gilt, dann gibt es einen Charakter χ, sodass gilt:

$$\chi(a) \neq 1.$$

Beweis:

Wir wissen, dass $\mathbb{F}_p^*$ zyklisch ist. Sei $g \in \mathbb{F}_p^*$ ein Erzeuger. Dann ist jedes $a \in F_p^*$ gleich einer Potenz von g. Falls $a = g^l$ und χ eine Charakter ist, dann gilt $\chi(a) = \chi(g)^l$. Dies zeigt, dass χ vollständig durch den Wert $\chi(g)$ bestimmt ist. Da $\chi(g)$ nach Satz 8.1.2 eine $(p-1)te$ Einheitswurzel ist, und da es genau $(p-1)$ Einheitswurzeln sind, folgt, dass die Charaktergruppe höchstens Ordnung $(p-1)$ hat.

$\chi \backslash a$	g	g^2	$\ldots$	g^{p-1}
ε	1			
λ	$e^{\frac{2\pi i}{p-1}}$			
λ^2	$e^{\frac{2\pi 2i}{p-1}}$			
$\vdots$				
λ^{p-1}	$e^{\frac{2\pi i(p-2)}{p-1}}$			

Aus der letzten Zeile folgt, dass genau $(p-1)$ verschiedene Charaktere existieren. Zudem wissen wir nach Satz 8.1.2 (b), dass $g^{(p-1)} = 1$. Dies ist wiederum das gleiche wie $(\chi(g))^{(p-1)} = 1$. Daraus folgt $\chi = e^{\frac{2\pi ik}{p-1}} = \lambda^k(g)$. □

Korollar 8.1.6:

Sei $a \in \mathbb{F}_p^*$ mit $a \neq 1$. Dann ist

$$\textstyle\sum_\chi \chi(a) = \varepsilon(a) + \lambda(a) + \lambda^2(a) + \ldots + \lambda^{(p-1)}(a) = 0$$

Beweis:

Sei $S = \sum_\chi \chi(a)$. Da $a \neq 1$ nach Voraussetzung gilt, gibt es einen Charakter λ, sodass $\lambda(a) \neq 1$. Dann ist

$$\lambda(a)S = \lambda(a)\sum_\chi \chi(a) = \sum_\chi \lambda(a)\chi(a) = \sum_\chi \lambda\chi(a) = S.$$

Die letzte Gleichheit gilt, da $\lambda\chi$ über alle Charaktere durchläuft, sofern χ alle Charaktere durchläuft. Wir erhalten also $(\lambda(a) - 1)S = 0$ und damit $S = 0$. □

Satz 8.1.7:

Sei $a \in \mathbb{F}_p^*$ und sei n eine natürliche Zahl so, dass $n|(p-1)$ und $x^n = a$ nicht lösbar ist. Dann gibt es einen Charakter χ, sodass

(a) $\chi^n = \varepsilon$

(b) $\chi(a) \neq 1$

Beweis:

Sei $g \in \mathbb{F}_p^*$ ein Erzeuger, sei λ wie im Beweis von Korollar 8.1.6 und sei n eine natürliche Zahl so, dass $n|(p-1)$ und $x^n = a$ nicht lösbar ist.

(a) Setze $\chi = \lambda^{\frac{(p-1)}{n}}$, $\{\chi^j | 1 \leq j \leq n\} = \{\lambda^{\frac{(p-1)}{n}}, \ldots, \lambda^{\frac{(p-1)}{n}(n-1)}, \varepsilon\}$. Daraus folgt $\chi^n = \lambda^{p-1} = \varepsilon$.

(b) Wir wissen $\chi(g) = e^{\frac{2\pi i}{n}}$ und damit wissen wir auch, dass $\chi^n(g) = 1$ ist. Nun sei $a = g^l$ für ein beliebiges l. Dann gilt

$$\chi(a) = \chi(g)^l = e^{\frac{2\pi i l}{n}}$$

Angenommen $\chi(a) = e^{\frac{2\pi i l}{n}} = 1$. Dann gilt $n|l$, also existiert ein l_1, sodass $l = nl_1$ ist. Dies bedeutet dann auch, dass $a = g^l = (g^{l_1})^n$, also dass $x = g^{l_1}$ eine Lösung ist. Widerspruch zur Voraussetzung, dass $x^n = a$ keine Lösung in $\mathbb{F}_p^*$ hat. Es folgt $\chi(a) \neq 1$.

□

Definition 8.1.8:

Für $a \in \mathbb{F}_p$ bezeichne $N(x^n = a)$ die *Anzahl der Lösungen* für $x^n = a$.

Satz 8.1.9

Sei $n|(p-1)$, dann ist $N(x^n = a) = \sum_{\chi^n = \varepsilon} \chi(a)$ die Summe über alle Charaktere, deren Ordnung n teilt.

Beweis:

Es sind im folgenden drei Fälle zu betrachten.

1. Fall: $a = 0$ (Sonderfall)
   Für $a = 0$ hat $x^n = 0$ nur eine Lösung, nämlich $x = 0$

2. Fall: $a \neq 0$ und $x^n = a$ ist lösbar:
   Das heißt, es existiert ein b so, dass $b^n = a$ gilt. Zunächst betrachten wir die rechte Seite der Gleichung $N(x^n = a) = \sum_{\chi^n = \varepsilon} \chi(a)$:

$$\sum_{\chi^n = \varepsilon} \chi(a) = \varepsilon(a) + \lambda^{\frac{(p-1)}{n}}(a) + \ldots + \lambda^{\frac{(p-1)}{n}(n-1)}(a).$$

   Ersetzte a nun durch b^n, dann erhält man:

$$= \underbrace{\varepsilon(b) + \varepsilon(b) + \ldots + \varepsilon(b)}_{n\text{-mal}} = n$$

   Nun betrachten wir die linke Seite der Gleichung

$$N(x^n = a) = n.$$

   Wir müssen also zeigen, dass die Anzahl der Lösungen n in $(\mathbb{F}_p^*, \cdot)$ ist. $(\mathbb{F}_p^*, \cdot)$ ist isomorph zu $(\mathbb{Z}_{p-1}, +)$ bzgl. einer Abbildung $\varphi : (\mathbb{F}_p^*, \cdot) \longrightarrow (\mathbb{Z}_{p-1}, +)$, wobei $(\mathbb{Z}_{p-1}, +) = \{0, 1, 2, \ldots, p-2\}$ und $n|(p-1)$. Sei $x^n = a$ in $\mathbb{F}_p^*$. Durch Anwenden von φ wird daraus $\varphi(x^n) = \varphi(a)$, also $n\varphi(x) = \varphi(a)$. Wir bezeichnen $\varphi(x) =: x_0$.

   Betrachte $\zeta_k = x_0 + \frac{p-1}{n}k$ für $k = 0, 1, \cdots, n-1$.

   Als erstes zeigen wir, dass ζ_k für $k = 0, 1, \cdots, n-1$ paarweise verschieden sind. Angenommen, $k_1 \neq k_2$. Dann gilt

$$x_0 + \frac{p-1}{n}k_1 = x_0 + \frac{p-1}{n}k_2$$

$$\iff \quad \frac{p-1}{n}k_1 = \frac{p-1}{n}k_2$$

$$\iff \quad \underbrace{\frac{p-1}{n}}_{\neq 0 \text{ für } p \neq 1} (k_1 - k_2) = 0$$

Daraus folgt $k_1 = k_2$ Widerspruch zu $k_1 \neq k_2$. Alle ζ_k für $k = 0, 1, \cdots, n-1$ sind paarweise verschieden. Es bleibt nun noch zu zeigen, dass ζ_k Lösungen sind. Es gilt

$$
\begin{aligned}
& n\zeta_k = \varphi(a) \\
\iff \quad & n\left(x_0 + \frac{p-1}{n}k\right) = \varphi(a) \\
\iff \quad & nx_0 + \underbrace{(p-1)k}_{=0} = \varphi(a) \quad \text{in } \mathbb{Z}_{p-1} \\
\iff \quad & nx_0 + \underbrace{(p-1)\,k}_{=0} = \varphi(a) \quad \text{in } \mathbb{Z}_{p-1} \\
\iff \quad & nx_0 = \varphi(a)
\end{aligned}
$$

Also sind ζ_k Lösungen der Gleichung $n\varphi(x) = \varphi(a)$.

3. Fall: Sei $a \neq 0$ und sei $x^n = a$ ist nicht lösbar.
Wir müssen zeigen, dass $\sum_{\chi^n=\varepsilon} \chi(a) = 0$. Setze

$$T := \sum_{\chi^n=\varepsilon} \chi(a)$$

Nach Satz 8.1.6 gibt es ein Charakter ρ, sodass $\rho(a) \neq 1$ und $\rho^n = \varepsilon$. Eine einfache Rechnung zeigt, dass $\rho(a)T = T$ ist. Hierbei benutzt man die offensichtliche Tatsache, dass der Charakter, deren Ordnung n teilt, eine Gruppe bildet. Damit gilt $(\rho(a) - 1)T = 0$, also $T = 0$.

□

Folgerung:

Als ein Spezialfall sei p prim und ungerade, $n = 2$. Dann besagt der Satz, dass $N(x^2 = a) = 1 + \left(\frac{a}{p}\right)$, wobei $\left(\frac{a}{p}\right)$ als Legendre Symbol aufzufassen ist.

Beweis

Zunächst ist zu zeigen: Die Charaktere $\chi = (\frac{\cdot}{p})$ und $\chi = \varepsilon$ lösen $\chi^2 = \varepsilon$. Denn $(\frac{\cdot}{p})$ ist ein Charakter mit $\mathbb{F}_p^* \longrightarrow \mathbb{C}^*$, $x \longmapsto \left(\frac{x}{p}\right) 5$, $xy \longmapsto \left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$
Daraus folgt:

$$\chi(g) = \pm 1 \; \forall g \in \mathbb{F}_p^* \implies (\chi(g))^2 = 1 = \varepsilon(g) \; \forall g \in \mathbb{F}_p^*$$

Des weiteren bleibt zu zeigen: Es gibt nur zwei Lösungen von $\chi^2 = \varepsilon$.
Sei g ein Erzeuger von $\mathbb{F}_p^*$. Dann ist χ durch $\chi(g)$ eindeutig bestimmt. Insbesondere ist

$$(\chi(g))^2 = \underbrace{\varepsilon(g)}_{=1} \text{ in } \mathbb{C}^*$$

Daraus folgt, dass $\chi(g) = 1 \vee \chi(g) = -1$. □

2 Gauß - Summe

In Kapitel 6 wurde die Gauß-Summe eingeführt. In der nachfolgenden Definition wird die Notation verallgemeinert.

Definition 8.2.1:

Sei χ ein Charakter auf $\mathbb{F}_p$ und $a \in \mathbb{F}_p$. Setze $g_a(\chi) := \sum_{t=0}^{p-1} \chi(t)\zeta^{at}$, wobei $\zeta = e^{\frac{2\pi i}{p}}$. $g_a(\chi)$ heißt die zu χ zugehörige *Gauß-Summe* von $\mathbb{F}_p$.

Satz 8.2.2:

(1) Falls $a \neq 0$ und $\chi \neq \varepsilon$, dann gilt $g_a(\chi) = \chi\left(a^{-1}\right) g_1(\chi)$.

(2) Falls $a \neq 0$ und $\chi = \varepsilon$, dann gilt $g_a(\varepsilon) = 0$.

(3) Falls $a = 0$ und $\chi \neq \varepsilon$, dann gilt $g_0(\chi) = 0$.

(4) Falls $a = 0$ und $\chi = \varepsilon$, dann gilt $g_0(\varepsilon) = p$.

$a\backslash\chi$	$\neq \varepsilon$	ε
$\neq 0$	$\chi\left(a^{-1}\right) g_1(\chi)$	0
0	0	p

Beweis:

(1) Sei $a \neq 0$ und $\chi \neq \varepsilon$, dann erhält man

$$\chi(a)g_a(\chi) = \chi(a)\sum_{t=0}^{p-1}\chi(t)\zeta^{at} = \sum_{t=0}^{p-1}\chi(at)\zeta^{at} = \sum_{t=0}^{p-1}\chi(t)\zeta^{t} = g_1(\chi)$$

(2) Sei $a \neq 0$ und $\chi = \varepsilon$ Mit Hilfe von Lemma 1 aus Kapitel 6 erhalten wir

$$g_a(\varepsilon) = \sum_{t=0}^{p-1}\varepsilon(t)\zeta^{at} = \sum_{t=0}^{p-1}\zeta^{at} = 0.$$

Um den Beweis zu beenden beachte

$$g_0(\chi) = \sum_{t=0}^{p-1}\chi(t)\zeta^{0t} = \sum_{t=0}^{p-1}\chi(t) \quad \text{für } a = 0.$$

(3) Sei $a = 0$ und $\chi \neq \varepsilon$, dann erhält man

$$g_0(\chi) = 0$$

nach Satz 8.1.3.

(4) Sei $a = 0$ und $\chi = \varepsilon$, dann erhält man

$$g_0(\varepsilon) = p$$

□

Von nun an bezeichnen wir $g_1(\chi)$ mit $g(\chi)$. Wir wollen den Absolutbetrag von $g(\chi)$ bestimmen. Dies kann man einfach analog zum Beweis 6.3.2 durchführen.

Satz 8.2.3:

Falls $\chi \neq \varepsilon$ ist, dann gilt $|g(\chi)| = \sqrt{p}$.

Beweis:

Idee: Berechne $\sum_a g_a(\chi)\overline{g_a(\chi)}$ auf zwei Wegen.

Falls $a \neq 0$, dann gilt nach Satz 8.1.2:

$$\overline{g_a(\chi)} = \overline{\chi(a^{-1})g(\chi)} = \chi(a)\overline{g(\chi)} \text{ und } g_a(\chi) = \chi(a^{-1})g(\chi)$$

Daraus folgt

$$g_a(\chi) = \overline{g_a(\chi)} = \chi\left(a^{-1}\right)\chi(a)g(\chi)\overline{g(\chi)} = |g(\chi)|^2$$

Da $g_0(\chi) = 0$ ist, hat die Summe den Wert $(p-1)|g(\chi)|^2$.
Andererseits ist

$$g_a(\chi)\overline{g_a(\chi)} = \sum_x \sum_y \chi(x)\overline{\chi(y)}\zeta^{ax-ay}$$

Summiert man beide Seiten über a und benutzt Korollar 1 aus Kapitel 6, so erhält man

$$\sum_a g_a(\chi)\overline{g_a(\chi)} = \sum_x \sum_y \chi(x)\overline{\chi(y)}\delta(x,y)p = (p-1)p$$

Daraus folgt

$$(p-1)|g(\chi)|^2 = (p-1)p$$

und daraus folgt die Behauptung. □