Jacobi Summen

Tobias Liebke

May 18, 2017

1 Motivation

Betrachte die Gleichung $x^2 + y^2 = 1$ im Körper $\mathbb{F}_p$. Da $\mathbb{F}_p$ endlich ist, gibt es nur endlich viele Lösungen dieser Gleichung. Sei nun $N(x^2+y^2 = 1)$ die Anzahl dieser Lösungen. Man sieht nun dass

$$N(x^2 + y^2 = 1) = \sum_{a+b=1} N(x^2 = a)N(y^2 = b)$$

wobei die Summe über alle $a, b \in \mathbb{F}_p \; mit \; a + b = 1$ läuft. Wir wissen aus dem vorherigen Paragraphen dass $N(x^2 = a) = 1 + (a/p)$. Einsetzen liefert also

$$N(x^2+y^2 = 1) = \sum_{a+b=1} (1+\left(\frac{a}{p}\right))(1+\left(\frac{b}{p}\right)) = p+\sum_a \left(\frac{a}{p}\right)+\sum_b \left(\frac{b}{p}\right)+\sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Die ersten beiden Summen sind 0 wie wir aus dem vorherigen Paragraphen wissen. Bleibt also die Aufgabe die letzte Summe zu berechnen.

Betrachte nun die Gleichung $x^3 + y^3 = 1$, auch hier wollen wir die Anzahl der Lösungen berechnen. Wie zuvor haben wir,

$$N(x^3 + y^3 = 1) = \sum_{a+b=1} N(x^3 = a)N(y^3 = b)$$

Ist nun $p \equiv 2(3)$ dann ist der $ggT(3, p-1) = 1$ und damit folgt, dass es für jedes $a \in \mathbb{F}_p$ nur eine Lösung gibt, also $N(x^3 = a) = 1$ ist. Daraus folgt direkt $N(x^3 + y^3 = 1) = p$

Betrachte nun also $p \equiv 1(3)$. Sei $\chi \neq \epsilon$ ein Character der Ordnung 3. Dann ist auch $\chi^2 \neq \epsilon$ von Ordnung 3. Nach Proposition 8.1.5. gilt also $N(x^3 = a) = 1 + \chi(a) + \chi^2(a)$. Durch Vertauschen der Summen folgt insgesamt:

$$N(x^3 + y^3 = 1) = \sum_{a+b=1} \sum_{i=0}^{2} \chi^i(a) \sum_{j=0}^{2} \chi^j(b) = \sum_{i=0}^{2} \sum_{j=0}^{2} (\sum_{a+b=1} \chi^i(a)\chi^j(b))$$

Die Innere Summe sieht aus, wie in $N(x^2 + y^2 = 1)$.

2 Die Jacobi Summe

Definition 1 *Seien χ und λ Charactere von $\mathbb{F}_p$, dann ist*

$$J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$$

die Jacobi Summe von χ und λ.

Um die genauen Werte für $N(x^2 + y^2 = 1)$ und $N(x^3 + y^3 = 1)$ zu bekommen betrachten wir nun die Werte der Jacobi Summe.

Theorem 1 *Seien χ und λ nicht-triviale Charactere von $\mathbb{F}_p$, dann ist*

$$(a)\ J(\epsilon, \epsilon) = p$$

$$(b)\ J(\epsilon, \chi) = 0$$

$$(c)\ J(\chi, \chi^{-1}) = -\chi(-1)$$

$$(d)\ Wenn\ \chi\lambda \neq \epsilon, dann\ J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$$

Beweis

$$(a)\ J(\epsilon, \epsilon) = \sum_{a+b=1} \epsilon(a)\epsilon(b) = \sum_{a+b=1} 1 = p$$

$$(b)\ J(\epsilon, \chi) = \sum_{a+b=1} \epsilon(a)\chi(b) = \sum_{a+b=1} \chi(b) = 0$$

$$(c)\ J(\chi, \chi^{-1)} = \sum_{\substack{a+b=1 \\ b\neq 0}} \chi(a)\chi^{-1}(b) = \sum_{\substack{a+b=1 \\ b\neq 0}} \chi\left(\frac{a}{b}\right) = \sum_{a\neq 1} \chi\left(\frac{a}{1-a}\right)$$

Setzen wir nun $c = \frac{a}{1-a}$ so haben wir $a = \frac{c}{1+c}$. Genauso wie a über $\mathbb{F}_p$ ohne die 1 läuft, so läuft c über $\mathbb{F}_p$ ohne die -1 . Insgesamt folgt also

$$J(\chi, \chi^{-1)} = \sum_{c\neq -1} \chi(c) = -\chi(-1)$$

Um nun (d) zu beweisen betrachten wir zunächst $g(\chi)g(\lambda)$

$$g(\chi)g(\lambda) = \left(\sum_x \chi(x)\zeta^x\right)\left(\sum_y \lambda(y)\zeta^y\right) = \sum_{x,y} \chi(x)\lambda(y)\zeta^{x+y} = \sum_t \left(\sum_{x+y=t} \chi(x)\lambda(y)\right)\zeta^t$$

Wenn $t = 0$ ist, dann ist $\sum_{x+y=0} \chi(x)\lambda(y) = \sum_x \chi(x)\lambda(-x) = \lambda(-1)\sum_x \chi\lambda(x) = 0$, da $\chi\lambda \neq \epsilon$ nach Voraussetzung.
Wenn $t \neq 0$ dann definieren wir x' und y', so dass $x = tx'$ und $y = ty'$. aus $x + y = t$ folgt dann $x' + y' = 1$. Insgesamt bekommen wir

$$\sum_{x+y=t} \chi(x)\lambda(y) = \sum_{x'+y'=1} \chi(tx')\lambda(ty') = \chi\lambda(t) \sum_{x'+y'=1} \chi(x')\lambda(y') = \chi\lambda(t)J(\chi,\lambda)$$

Setzen wir dies nun in die obige Gleichung ein erhalten wir:

$$g(\chi)g(\lambda) = \sum_t \chi\lambda(t)J(\chi,\lambda)\zeta^t = J(\chi,\lambda)g(\chi\lambda)$$

□

Korollar 1 *Seinen χ, λ und $\chi\lambda$ alle ungleich ϵ dann ist $|J(\chi,\lambda)| = \sqrt{p}$*

Beweis Nimmt man die absolut Beträge beider Seiten aus Theorem 1(d) sowie $|g(\chi)| = \sqrt{(}p)$.(nach Prop 8.2.2), so erhält man dies. □

Nun zurück zu $N(x^2 + y^2 = 1)$ und $N(x^3 + y^3 = 1)$, im ersten Fall erhalten wir durch Theorem 1(c) und den Reziprozitätssatz,

$$N(x^2+y^2=1) = p + \sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = p + \sum_a \left(\frac{a}{p}\right)\left(\frac{1-a}{p}\right) = p - \left(\frac{-1}{p}\right) = p - (-1)^{\frac{p-1}{2}}$$

Im zweiten Fall erhalten wir durch ausmultiplizieren und Anwedung von Theorem 1:

$$N(x^3 + y^3 = 1) = p - \chi(-1) - \chi^2(-1) + J(\chi,\chi) + J(\chi^2,\chi^2)$$

Es ist $\chi(-1) = \chi^3(-1) = 1$ und $\chi^2 = \chi^{-1} = \bar{\chi}$, daraus folgt:

$$N(x^3 + y^3 = 1) = p - 2 + 2Re\ J(\chi,\chi)$$

Eine klare Lösung ist dies nicht, da wir den Wert von $J(\chi,\chi)$ nicht explizit kennen. Aber aus Korollar 1 können wir zumindest eine Näherung bestimmen

$$|N(x^3 + y^3 = 1) - p + 2| \leq 2\sqrt{p}$$

Also gibt es für jede Primzahl p, näherungsweise $p - 2$ Lösungen, allerdings mit einem Fehlerwert von $\pm 2\sqrt{p}$. Wir haben also eine Näherung erhalten, unser Ziel bleibt es, eine konkrete Lösung ausrechnen zu können.

Aus Korollar 1 folgt nun

Proposition 1 *(a) Ist $p \equiv 1(4)$, dann existieren $a, b \in \mathbb{Z}$, so dass $a^2 + b^2 = p$.*
(b) Ist $p \equiv 1(3)$, dann existieren $a, b \in \mathbb{Z}$, so dass $a^2 - ab + b^2 = p$

Beweis Zu (a), da $p \equiv 1(4)$ ist, existiert ein Character der Ordnung 4. Die Werte dieses Characters sind $\{1, -1, i, -i\}$. Also gilt für die Jacobi Summe $J(\chi, \chi) = \sum_{s+t=1} \chi(s)\chi(t)$, dass sie aus dem Ring $\mathbb{Z}$[i] ist. Daher ist $J(\chi, \chi) = a + bi$ wobei $a, b \in \mathbb{Z}$. Insgesamt also:

$$p = |J(\chi, \chi)|^2 = |a + bi|^2 = a^2 + b^2$$

Bei (b) argumentieren wir genauso, da $p \equiv 1(3)$ ist, muss ein Character der Ordnung 3 existieren. Dieser nimmt die Werte $\{1, \omega, \omega^2\}$ an, wobei $\omega = -1/2 + \sqrt{-3}/2$. Analog zu (a) bedeutet dies, dass $J(\chi, \chi) \in \mathbb{Z}[\omega]$. Also ist $J(\chi, \chi) = a + b\omega$ mit $a, b \in \mathbb{Z}$. Insgesamt also:

$$p = |J(\chi, \chi)|^2 = |a + b\omega|^2 = a^2 - ab + b^2$$

□

Proposition 2 *Ist $p \equiv 1(3)$, dann existieren A, $B \in \mathbb{Z}$, so dass $4p = A^2 + 27B^2$ wobei $4p$, A und B eindeutig bis auf Vorzeichen sind.*

Beweis Aus Proposition 1 wissen wir, dass $p = a^2 - ab + b^2$ multiplizieren wir mit 4 so erhalten wir $4p = 4a^2 - 4ab + 4b^2$. Umformungen liefern nun, dass $4p = (2a - b)^2 + 3b^2 = (2b - a)^2 + 3a^2 = (a + b)^2 + 3(a - b)^2$.
Wir wollen nun zeigen, dass einer der drei Ausdrücke a, b oder (a-b) durch drei teilbar ist und wir somit 3^2 ausklammern können. Falls $3 \mid a$ oder $3 \mid b$ wären wir fertig. Also $3 \nmid a$ und $3 \nmid b$. Haben nun $a/3$ und $b/3$ verschiedene Reste o.B.d.A $a \equiv 1(3)$ und $b \equiv 2(3)$, dann wäre $a^2 - ab + b^2 \equiv 0(3)$ was bedeutet das $3 \mid p$, dies ist ein Widerspruch, da p eine Primzahl ist. Also haben a und b den gleichen Rest mod 3. Dies bedeutet, dass $(a - b) \equiv 0(3)$. Wir können also 3^2 ausklammern und erhalten so obige eindeutige Gleichung. □

Proposition 3 *Sei $p \equiv 1(n)$ und χ ein Character mit Ordnung $n > 2$, dann ist*

$$g(\chi)^n = \chi(-1)pJ(\chi, \chi)J(\chi, \chi^2) \cdots J(\chi, \chi^{n-2})$$

Beweis Aus Theorem 1 (d) wissen wir $g(\chi)^2 = J(\chi, \chi)g(\chi^2)$. Multiplizieren wir nun beide Seiten mit $g(\chi)$ erhalten wir $g(\chi)^3 = J(\chi, \chi)J(\chi, \chi^2)g(\chi^3)$ Dies sieht man leicht indem man die Jacobi Summen ausrechnet. Führt man dies nun weiter erhält man

$$g(\chi)^{n-1} = J(\chi, \chi)J(\chi, \chi^2) \cdots J(\chi, \chi^{n-2})g(\chi^{n-1})$$

Nun ist $\chi^{n-1} = \chi^{-1} = \bar{\chi}$ und damit ist $g(\chi)g(\chi^{n-1}) = g(\chi)g(\bar{\chi}) = -\chi(-1)p$. Multiplizieren wir also die obige Gleichung nochmal mit $g(\chi)$ so erhalten wir die Behauptung. □

Korollar 2 *Wenn χ ein kubischer Character ist, so gilt $g(\chi)^3 = pJ(\chi,\chi)$*

Beweis Dies ist lediglich der Spezialfall der Proposition für den Fall $n = 3$. Ausserdem ist $\chi(-1) = \chi((-1)^3) = 1$. □

Proposition 4 *Sei $p \equiv 1(3)$ und χ ein kubischer Character. $J(\chi,\chi) = a + b\omega$ wie vorher, dann ist*

$$(a)\ b \equiv 0(3)$$

$$(b)\ a \equiv -1(3)$$

Beweis Wir beweisen diese Proposition indem wir mit Kongruenzen im Ring algebraischer Integer arbeiten:

$$g(\chi)^3 = \left(\sum_t \chi(t)\zeta^t\right)^3 \equiv \sum_t \chi(t)^3\zeta^{3t}(3) = \sum_{t\neq 0} \zeta^{3t} = -1$$

Dies folgt da $\chi(0) = 0$ und $\chi(t)^3 = 1$ für $t \neq 0$. Insgesamt also für χ und $\bar{\chi}$:

$$g(\chi)^3 = pJ(\chi,\chi) \equiv a + b\omega \equiv -1(3)$$

$$g(\bar{\chi})^3 = pJ(\bar{\chi},\bar{\chi}) \equiv a + b\bar{\omega} \equiv -1(3)$$

Substraktion beider Gleichungen liefert nun $b(\omega - \bar{\omega}) \equiv 0(3)$ oder $b\sqrt{-3} \equiv 0(3)$, also folgt $-3b^2 \equiv 0(9)$, daraus folgt direkt $3 \mid b$. Da $3 \mid b$ und $a + b\omega \equiv -1(3)$, ist a $\equiv -1(3)$. □

Korollar 3 *Sei $p \equiv 1(3)$ und $A = 2a - b$ und $B = b/3$ mit $a, b \in \mathbb{Z}$, dann ist $A \equiv 1(3)$ und*

$$4p = A^2 + 27B^2$$

Beweis Wir wissen aus Proposition 1, dass $J(\chi,\chi) = a + b\omega$ und $|J(\chi,\chi)|^2 = p$, also $p = a^2 - ab + b^2$. Damit ist $4p = (2a - b)^2 + 3b^2$ und nach Proposition 2 $4p = A^2 + 27B^2$. Nach Proposition 4 ist $b \equiv 0(3)$ und $a \equiv -1(3)$ und somit $A = 2a - b \equiv 1(3)$. □

Theorem 2 *Sei $p \equiv 1(3)$, dann exisiteren $A, B \in \mathbb{Z}$, so dass $4p = A^2 + 27B^2$. Wenn wir voraussetzen, dass $A \equiv 1(3)$, dann ist A eindeutig bestimmt und*

$$N(x^3 + y^3 = 1) = p - 2 + A$$

Beweis Wir wissen bereits, dass $N(x^3+y^3 = 1) = p-2+2ReJ(\chi,\chi)$. Da $J(\chi,\chi) = a+b\omega$, ist der Realteil von $J(\chi,\chi) = (2a - b)/2$, also folgt $2\,Re\,J(\chi,\chi) = 2a - b = A \equiv 1(3)$. □

Wir wollen dies nun noch an zwei Beispielen zeigen. Wir nehmen hier die Fälle $p = 61$ und $p = 67$.
Im ersten Fall gilt $4 \cdot 61 = 1^2 + 17 \cdot 3^2$, also ist $N(x^3 + y^3 = 1) = 61 - 2 + 1 = 60$ in $\mathbb{F}_{61}$.
Im zweiten Fall ist $4 \cdot 67 = 5^2 + 17 \cdot 3^2$, da $5 \not\equiv 1(3)$, ist $A = -5$, also ist $N(x^3 + y^3 = 1) = 67 - 2 - 5 = 60$ in $\mathbb{F}_{67}$.