10. Abzählungen mod p

Um später die p-adischen Integrale auszurechnen, zählen wir Vektoren mod p auf Sphären und orthogonale Transformationen mod p. In diesem Kapitel sei $p \neq 2$ und zuerst

$\rho \neq 0$

Ein zweidimensionaler Vektorraum E über $\mathbb{F}_p$ ist entweder eine hyperbolische Ebene oder (als Vektorraum) isomorph zur quadratischen Erweiterung $\mathbb{F}_p(\sqrt{d})$ über $\mathbb{F}_p$ mit der Normform $x^2 - dy^2$. Dabei ist d ein Nichtquadrat in $\mathbb{F}_p$. Für die Anzahl $A(E,\rho)$ der Vektoren $x \in E$ mit $(x,x) = \rho$ findet man

$$A(E,\rho) = \begin{cases} p-1 & \text{wenn } E \text{ hyperbolisch} \\ p+1 & \text{wenn } E \text{ anisotrop} \end{cases} \tag{1}$$

denn die hyperbolische Form kann auf $(x,x) = x_1x_2$ transformiert werden, und die Norm ist ein Homomorphismus von $\mathbb{F}_{p^2}^*$ auf $\mathbb{F}_p^*$, ihr Kern hat also $p+1$ Elemente. Für die Darstellung der 0 findet man

$$A(E,0) = \begin{cases} 2p-1 & \text{wenn } E \text{ hyperbolisch} \\ 1 & \text{wenn } E \text{ anisotrop} \end{cases}$$

Jeder mindestens dreidimensionale Raum über $\mathbb{F}_p$ stellt 0 dar, von ihm kann man also eine hyperbolische Ebene abspalten. Ist nun $V = U \perp H$ und H hyperbolisch, so ist

$$A(V,\rho) = \sum_{\mu} A(U,\mu)A(H,\rho-\mu)$$

$$= (2p-1)A(U,\rho) + \sum_{\mu\neq\rho}(p-1)A(U,\mu) = p\cdot A(U,\rho) + (p-1)p^{n-2}$$

Um eine Rekursion zu haben, schreiben wir vorübergehend $A(n,\rho)$ statt $A(V,\rho)$. Dann haben wir

$$A(n,\rho) = p\cdot A(n-2,\rho) + (p-1)p^{n-2}$$

Dasselbe gilt für $n-2i$ anstelle von n, solange $n-2i \geq 3$:

$$A(n-2i,\rho) = p\cdot A(n-2i-2,\rho) + (p-1)p^{n-2i-2}$$

Diese Gleichung multiplizieren wir mit p^i und summieren über $i = 0, ..., k$:

$$A(n,\rho) = p^{k+1}A(n-2k-2,\rho) + p^{n-1} - p^{n-k-2} \tag{2}$$

Dies funktioniert, solange $n-2k-2 \geq 1$, also $2k \leq n-3$.

1. Fall: n gerade: Man schreibt

$$V = H \perp ..... \perp H \perp E \quad (H \text{ hyperbolisch, dim } E = 2)$$

Man nimmt $k = \frac{n}{2} - 2$ und erhält

$$A(n,\rho) = p^{\frac{n}{2}-1}A(2,\rho) + p^{n-1} - p^{\frac{n}{2}} \tag{3}$$

Mit $A(2,\rho)$ ist natürlich $A(E,\rho)$ gemeint, nach (1) also $p-1$ oder $p+1$, je nachdem ob E hyperbolisch oder anisotrop ist. Nun ist

$$E \text{ hyperbolisch } \Leftrightarrow -\det E \text{ Quadrat } \Leftrightarrow (-1)^{\frac{n}{2}} \det V \text{ Quadrat}$$

Wir können einheitlich schreiben

$$A(E,\rho) = p - \epsilon \text{ mit } \epsilon = (\frac{(-1)^{\frac{n}{2}} \det V}{p})$$

Setzt man dies in (3) ein, so erhält man

$$A(V,\rho) = p^{n-1} - \epsilon p^{\frac{n}{2}-1} \tag{4}$$

2. Fall: n ungerade. Jetzt schreibt man

$$V = H \perp ..... \perp H \perp \mathbb{F}_p e$$

und nimmt $k = \frac{n-3}{2}$. Dann erhält man

$$A(V,\rho) = p^{\frac{n-1}{2}} A(\mathbb{F}_p e,\rho) + p^{n-1} - p^{\frac{n-1}{2}}$$

Offensichtlich ist

$$A(\mathbb{F}_p e,\rho) = \begin{cases} 2 & \text{wenn } \rho(e,e) \text{ Quadrat} \\ 0 & \text{sonst} \end{cases}$$

Bis auf ein Quadrat ist (e,e) gleich $(-1)^{\frac{n-1}{2}} \det V$. Setzen wir

$$\epsilon' = (\frac{(-1)^{\frac{n-1}{2}} \rho \det V}{p})$$

so erhalten wir

$$A(V,\rho) = p^{n-1} + \epsilon' p^{\frac{n-1}{2}} \tag{5}$$

Jetzt wollen wir auch noch die isotropen Vektoren zählen (also die $x \neq 0$ mit $(x,x) = 0$). Die Formel (2) gilt kraft ihrer Herleitung auch für $\rho = 0$. Bei geradem n benutzen wir sie für $k = \frac{n}{2} - 2$. Die Anzahl *aller* $x \in V$ mit $(x,x) = 0$ ist

$$A(V,0) = p^{\frac{n}{2}-1} A(E,0) + p^{n-1} - p^{\frac{n}{2}}$$

und

$$A(E,0) = \begin{cases} 1 & \text{wenn } E \text{ anisotrop , das heiß } \epsilon = -1 \\ 2p-1 & \text{wenn } E \text{ hyperbolisch, das heißt } \epsilon = 1 \end{cases}$$

Das ergibt

$$A(V,0) = \begin{cases} p^{\frac{n}{2}-1} + p^{n-1} - p^{\frac{n}{2}} & \text{wenn } E \text{ anisotrop} \\ p^{\frac{n}{2}} - p^{\frac{n}{2}-1} + p^{n-1} & \text{wenn } E \text{ hyperbolisch} \end{cases}$$

Die Zahl $A^*(V,0)$ der isotropen Vektoren ist 1 weniger. Unter Benutzung von ϵ kann man sie einheitlich schreiben:

$$A^*(V,0) = (p^{\frac{n}{2}} - \epsilon)(p^{\frac{n}{2}-1} + \epsilon)$$

Für ungerades n folgt aus $A(1,0) = 1$, daß $A(n,0) = p^{n-1}$. also

$$A^*(V,0) = p^{n-1} - 1$$

Mit Hilfe dieser Formeln können wir zählen, wie viele orthogonale Transformationen V gestattet. Dazu nehmen wir eine Orthogonalbasis $e_1, ..., e_n$ von V über $\mathbb{F}_p$, mit $(e_i, e_i) =: \alpha_i$. Für jede orthogonale Transformation T ist $(Te_1, Te_1) = \alpha_1$. Umgekehrt: Wenn $(x,x) = \alpha_1$, dann gibt es eine orthogonale Transformation T mit $x = Te_1$, und solange $\dim V \geq 2$, kann $\det T = 1$ genommen werden. Daraus folgt: Wenn $G(V)$ die spezielle orthogonale Gruppe ist, dann gilt

$$|G(V)| = A(V, \alpha_1) \cdot |G(\mathbb{F}_p e_2 \perp ..... \perp \mathbb{F}_p e_n)|$$

Setzt man $V_i = \mathbb{F}_p e_{i+1} \perp ..... \perp \mathbb{F}_p e_n$, so folgt rekursiv

$$|G(V)| = A(V_0, \alpha_1)A(V_1, \alpha_2).....A(V_{n-2}, \alpha_{n-1})|G(\mathbb{F}_p e_n)|$$

und der letzte Faktor ist 1. Aus den Formeln 4 und 5 erhalten wir

$$A(V_{n-2}, \alpha_{n-1}) = p - (\frac{-\alpha_{n-1}\alpha_n}{p})$$

$$A(V_{n-3}, \alpha_{n-2}) = p^2 + (\frac{-\alpha_{n-1}\alpha_n}{p})p$$

$$A(V_{n-4}, \alpha_{n-3}) = p^3 - (\frac{\alpha_{n-3}\alpha_{n-2}\alpha_{n-1}\alpha_n}{p})p$$

$$A(V_{n-5}, \alpha_{n-4}) = p^4 + (\frac{\alpha_{n-3}\alpha_{n-2}\alpha_{n-1}\alpha_n}{p})p^2$$

Wenn n ungerade ≥ 3 ist, hat man am Ende

$$A(V_1, \alpha_2) = p^{n-2} - (\frac{(-1)^{\frac{n-1}{2}}\alpha_2.....\alpha_n}{p})p^{\frac{n-1}{2}-1}$$

$$A(V_0, \alpha_1) = p^{n-1} + (\frac{(-1)^{\frac{n-1}{2}}\alpha_2.....\alpha_n}{p})p^{\frac{n-1}{2}}$$

Hier kann man die Faktoren paarweise zusammenfassen und erhält

$$|G(V)| = p^{1+2+....+(n-1)}(1-p^{-2})(1-p^{-4}).....(1-p^{-(n-1)}) \tag{6}$$

Wenn n gerade ist, dann bleibt V_0 übrig, und man erhält

$$|G(V)| = p^{1+2+....+(n-1)}(1-p^{-2})(1-p^{-4}).....(1-p^{-(n-2)})(1-(\frac{(-1)^{\frac{n}{2}}\det V}{p})p^{-\frac{n}{2}}) \tag{7}$$