Kleines p oder q

Philipp Niemann

15. Januar 2009

Schriftliche Ausarbeitung zum Vortrag im Rahmen des Seminars AlZAGK
Prof.'en Gamst, Hortmann, Oeljeklaus
Universität Bremen, WS 2008/09

Zusammenfassung

Nach einiger Vorarbeit zum Beweis der Catalanschen Vermutung, dass die Gleichung

$$x^p - y^q = 1 \tag{1}$$

in ganzen Zahlen ohne Null nur eine Lösung hat, wissen wir bereits, dass wir uns für p und q auf ungerade, verschiedene Primzahlen beschränken können.

Mit den Resultaten von Cassels und einem Exkurs in die p-adischen Zahlen leiten wir für hypothetische weitere Lösungen der obigen Gleichung eine untere Schranke für p und q her, die für sich genommen keine große Bedeutung hat, aber im weiteren Verlauf von Mihailescus Beweis eine hilfreiche Abschätzung liefert.

Obgleich ein ähnliches Resultat zuvor bereits mit anderen Methoden erzielt wurde, orientieren wir uns an dem von René Schoof skizzierten, auf Kreisteilungskörpern basierenden Beweis in [Schoof], Kapitel 8.

1 Setting

In diesem Kapitel erinnern wir uns an den Kontext der Kreisteilungskörper, gebräuchliche Notationen und bereits im Vorfeld erzielte Ergebnisse und skizzieren den angestrebten Widerspruchsbeweis zur Formulierung einer unteren Schranke für die Exponenten p und q von hypothetischen Lösungen der Catalanschen Gleichung.

Seien p, q verschiedene, ungerade Primzahlen, $x, y \in \mathbb{Z} - \{0\}$ eine Lösung der Catalanschen Gleichung (1). Zu einer komplexen p-ten Einheitswurzel $\zeta_p \neq 1$ betrachten wir den p-ten Kreisteilungskörper $F = \mathbb{Q}(\zeta_p)$, den Ring $\mathcal{O}_F = \mathbb{Z}[\zeta_p]$ der ganzen Zahlen in F, die Klassengruppe Cl_p mit endlicher Klassenzahl $h_p = |Cl_p|$. Es bezeichne $\iota \in G = \mathrm{Gal}(F/\mathbb{Q})$ die komplexe Konjugation.

Weiterhin sei $F^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ der größte reelle Teilkörper von F, Cl_p^+ seine Klassengruppe. Aus der Theorie der Kreisteilungskörper ist bekannt, dass $Cl_p^- = Cl_p/Cl_p^+$ endlich ist und dass $h_p^- = |Cl_p^-|$ für kleine p bereits konkret ausgerechnet wurde. Eine Tabelle mit diesen Zahlen findet man z.B. in [LWash].

Definiere $\pi := \zeta_p - 1$. Damit ist (π) ein Primideal und es gilt $(p) = (\pi)^{p-1}$. Wir greifen zurück auf die Hindernisgruppe

$$H := \{\alpha \in \mathbb{Q}^*(\zeta_p) | (\alpha) = \mathcal{A}^q \cdot (\pi)^k, k \in \mathbb{Z}, \mathcal{A} \text{ gebr. Ideal}\}/\mathbb{Q}^*(\zeta_p)^q$$

Die Klasse von $x - \zeta_p$ liegt in H, welches als $\mathbb{F}_q[G]$-Modul eine Zerlegung $H = H^+ \oplus H^-$ besitzt mit $H^- = H^{1-\iota} \cong Cl_p^-[q]$.

Wir werden zeigen, dass das zu einer hypothetischen Lösung gehörende Element $(x-\zeta_p)^{1-\iota} \in H^-$ nicht-trivial ist, was für bestimmte p und q im Widerspruch dazu stehen wird, dass Cl_p^- gar keine nicht-trivialen q-primären Elemente enthält.

2 Konstruktion einer Einheit

Die Annahme, dass das zu einer hypothetischen Lösung der Catalanschen Gleichung assoziierte Element $(x-\zeta_p)^{1-\iota}$ der Hindernisgruppe trivial ist, lässt die Konstruktion einer Einheit in $\mathbb{Q}(\zeta_p)$ zu, die allerdings der p-adischen Betrachtung im nächsten Kapitel nicht standhalten kann.

Nehmen wir also an, dass $(x-\zeta_p)^{1-\iota}$ trivial in H^- ist, das bedeutet, dass $\frac{x-\zeta_p}{x-\overline{\zeta_p}} = \alpha^q$ für ein $\alpha \in \mathbb{Q}^*(\zeta_p)$. Sei $w \in \overline{\mathbb{Q}}$ (algebraischer Abschluss) eine q-te Wurzel von $\frac{x-\zeta_p}{1-\zeta_p} \in \mathbb{Q}(\zeta_p)$. Mit $w' = \frac{w}{\alpha}$ haben wir dann eine q-te Wurzel von $\frac{x-\overline{\zeta_p}}{1-\zeta_p}$.
Wir setzen

$$\eta := (w-w')^q = w^q \cdot \left(1-\frac{1}{\alpha}\right)^q = \frac{x-\zeta_p}{1-\zeta_p} \cdot \left(1-\frac{1}{\alpha}\right)^q$$

und stellen fest, dass η unabhängig von der Wahl der q-ten Wurzel w ist und a priori nur in $\mathbb{Q}(\zeta_p)$ ist.
Bevor wir zeigen, dass η sogar eine Einheit ist, machen wir uns zwei einfache Tatsachen aus der Zahlentheorie klar:

Lemma 2.1. .

(1) Ist a ganz über $\mathbb{Z}$, dann auch $\sqrt[n]{a}$ für natürliches n.

(2) für $r \in \mathbb{Z}, (r,p) = 1$ ist $1+\zeta_p^r$ eine Einheit im p-ten Kreisteilungskörper $\mathbb{Q}(\zeta_p)$.

Beweis. .

(1) trivial

(2) $1+\zeta_p^r = (1+\zeta_p^r) \cdot \frac{1-\zeta_p^r}{1-\zeta_p^r} = \frac{1-\zeta_p^{2r}}{1-\zeta_p^r} \in \mathbb{Z}^*[\zeta_p]$, weil $(2r^2, p) = 1$
(Lemma aus der Kreisteilungstheorie)

□

Damit lässt sich die folgende Proposition zeigen:

Proposition 2.2. *(vgl. Schoof: Proposition 8.1)*

(i) η ist eine Einheit

(ii) die Norm (von $\mathbb{Q}(\zeta_p)$ nach $\mathbb{Q}$) von η ist gleich 1

Beweis. .

(i) Wir beobachten, dass

$$\begin{aligned}\frac{x-\zeta_p}{1-\zeta_p} &= \frac{x-1}{1-\zeta_p}+1 \\ &= \frac{k\cdot p^{q-1}}{1-\zeta_p}+1 && \text{| Cassels: } x\equiv 1 \bmod p^{q-1} \\ &= \frac{k\cdot \pi^{(p-1)\cdot(q-1)}\cdot\epsilon}{\pi}+1 && \text{|vgl. Setting} \\ &= k\cdot\pi^{(p-1)\cdot(q-1)-1}\cdot\epsilon+1\end{aligned}$$

für ein $\epsilon\in\mathbb{Z}^*[\zeta_p], k\in\mathbb{Z}$. Also ist $\frac{x-\zeta_p}{1-\zeta_p}$ ganz und damit nach dem vorangegangenen Lemma auch die q-te Wurzel w ganz.
Analog erhält man, dass w' ganz ist und somit auch $\eta=(w-w')^q$.

Weiterhin gilt die folgende Gleichung ganzer Zahlen (ganz über $\mathbb{Z}$):

$$\begin{aligned}(w-w')\cdot\sum_{k=0}^{q-1}w^k\cdot(w')^{q-1-k} = w^q-w'^q &= \frac{x-\zeta_p}{1-\zeta_p}-\frac{x-\overline{\zeta_p}}{1-\zeta_p} \\ &= \frac{\zeta_p^{-1}-\zeta_p}{1-\zeta_p}=\frac{(1-\zeta_p)(1+\zeta_p^{-1})}{1-\zeta_p} \\ &= 1+\zeta_p^{-1}\end{aligned}$$

Nach dem Lemma ist die letzte Zahl eine Einheit. Somit müssen auch $w-w'$ und η Einheiten sein.

(ii) Die Körpernorm einer Einheit ist gleich ±1. Da $N(\eta)$ zugleich ein Produkt von Paaren komplex Konjugierter ist, muss $N(\eta)=1$ gelten.

□

3 Widerspruch im p-adischen

Die Norm der eben konstruierten Einheit η wird im folgenden Kapitel p-adisch berechnet und mit dem im vorhergehenden Kapitel erzielten Ergebnis konfrontiert, dass $N(\eta)=1$.

Tragen wir zunächst ohne Beweis einige Fakten über die p-adischen Zahlkörper $\mathbb{Q}_p$ (für p Primzahl) zusammen. Für eine ausführliche Behandlung dieses Themas konsultiere man z.B. [Neukirch].

3.1 Exkurs: p-adische Zahlen

Die p-adischen ganzen Zahlen $\mathbb{Z}_p$ lassen sich auffassen als Unterring des unendlichen direkten Produktes $R=\prod_{n=1}^{\infty}(\mathbb{Z}/p^n\mathbb{Z})$ mit komponentenweise definierten Operationen, vermöge

$$\mathbb{Z}_p=\{(x_n)\in R \mid \text{für } 1\le k,l: x_{k+l}+p^k\mathbb{Z}=x_k+p^k\mathbb{Z}\}$$

Diese Forderung besagt, dass die natürliche Projektion der $(k+l)$-ten Komponente in die k-te Komponente die gleiche Restklasse liefert. [Man nennt diese Konstruktion auch „projektiver Limes“.]

Durch die Identifikation einer ganzen Zahl a mit der Folge $(a+p^n\mathbb{Z})_{n\in\mathbb{N}}$ lässt sich $\mathbb{Z}$ und auf ähnliche Weise sogar $\mathbb{Z}_{(p)}=\{\frac{g}{h}\in\mathbb{Q}|(p,h)=1\}$ als Teilmenge

von $\mathbb{Z}_p$ auffassen.
$\mathbb{Z}_p$ hat nur ein maximales Ideal, nämlich das von p erzeugte und $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$. Man erhält also die p-adischen Zahlen $\mathbb{Q}_p$ aus $\mathbb{Z}_p$, indem p invertierbar gemacht wird. Also hat jedes $f \in \mathbb{Q}_p$ eine Darstellung $f = p^{-m} \cdot g, g \in \mathbb{Z}_p, m \in \mathbb{N}$.

Andererseits besitzt jedes $x \in \mathbb{Q}, x \neq 0$ eine Darstellung $x = p^k \cdot \frac{g}{h}$, wobei $(gh, p) = 1, k \in \mathbb{Z}$. Setzt man $|x|_p = p^{-k}$, erhält man auf $\mathbb{Q}$ den sogenannten p-adischen Absolutbetrag, der ultrametrisch ist, d.h. die verschärfte Dreiecksungleichung $\forall x, y \in \mathbb{Q}^* : |x + y|_p \leq max(|x|_p, |y|_p)$ erfüllt. Der Exponent k definiert die p-adische Exponentialbewertung $\nu_p(x)$. Die Vervollständigung von $\mathbb{Q}$ über Cauchy-Folgen der von diesem Betrag induzierten Metrik liefert ebenfalls die p-adischen Zahlen $\mathbb{Q}_p$. Aufgrund der ultrametrischen Ungleichung konvergieren Reihen hier anders als im Reellen bereits dann, wenn die Summanden eine Nullfolge bilden.

3.2 q-te (Einheits-)Wurzeln im p-adischen

Während wir bei der Konstruktion der Einheit η auf wenig greifbare q-te Wurzeln zurückgreifen mussten, können wir uns im p-adischen zunutze machen, dass wir zumindest eine q-te Wurzel konkret formelmäßig angeben können.

Betrachten wir nun also die Körpererweiterung $\mathbb{Q}_p(\zeta_p)$ über $\mathbb{Q}_p$. Weil ζ_p über $\mathbb{Q}_p$ dasselbe Minimalpolynom besitzt wie über $\mathbb{Q}$, gilt

$$|\mathbb{Q}_p(\zeta_p) : \mathbb{Q}_p| = p - 1 = |\mathbb{Q}(\zeta_p) : \mathbb{Q}|.$$

Daher lässt sich diese Körpererweiterung der Vervollständigung $\mathbb{Q}_p$ mit der Vervollständigung der zuvor betrachteten Körpererweiterung $\mathbb{Q}(\zeta_p)$ identifizieren, so dass auch hier - unter den getroffenen Annahmen - $N(\eta) = 1$ gelten muss.

Aus der reellen Analysis ist für die binomische Reihe bekannt, dass

$$(1 + x)^{\frac{1}{q}} = \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} x^j \text{ für } |x| < 1.$$

Die Reihe konvergiert p-adisch bereits für $x \in p\mathbb{Z}_p$, da

$$\nu_p\left(\binom{\frac{1}{q}}{j} x^j\right) \geq j - \nu_p(j!) \geq (1 - \frac{1}{p-1})j$$

(vgl. [Neukirch], Kaptitel II, Lemma 5.6) über alle Grenzen wächst, wenn nur j über alle Grenzen wächst, und somit die Summanden absolut betrachtet eine Nullfolge bilden.

Setze nun $\mu := \frac{x-1}{1-\zeta_p}$, so dass

$$w^q = \frac{x - \zeta_p}{1 - \zeta_p} = 1 + \mu \text{ und } w'^q = \frac{x - \overline{\zeta_p}}{1 - \zeta_p} = -\overline{\zeta_p} \cdot \frac{x - \overline{\zeta_p}}{1 - \overline{\zeta_p}} = -\zeta_p^{-1} \cdot (1 + \overline{\mu}),$$

und wähle als q-te Wurzel $w = \sqrt[q]{1 + \mu} = \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \mu^j \in \mathbb{Z}_p[\zeta_p]$.

Die Reihe konvergiert, weil nach Cassels $x \equiv 1(p^{q-1})$, also:

$$\mu = \frac{x - 1}{1 - \zeta_p} = \frac{k \cdot p}{\pi} \cdot p^{q-2} = k \cdot \epsilon \cdot \pi^{p-2} \cdot p^{q-2} \equiv 0 \ (p^{q-2})$$

Man muss einen gewissen Aufwand mit q-ten Einheitswurzeln in $\mathbb{Q}_p(\zeta_p)$ treiben, um zu zeigen, dass tatsächlich

$$w' = \frac{w}{\alpha} = -\zeta_p^r \cdot \sqrt[q]{1 + \overline{\mu}} = -\zeta_p^r \cdot \sum_{j=0}^{\infty} \binom{\frac{1}{q}}{j} \overline{\mu}^j, \text{ mit } r \in \mathbb{Z}, rq \equiv -1 \ (p) \text{ gilt.}$$

Das würde hier allerdings den Rahmen sprengen, so dass wir auf den Beweis verzichten und überdies die folgende Proposition, deren Beweis ganz ähnlich zu dem weiter unten vorgeführten verläuft, hinnehmen:

Proposition 3.1. *(vgl. Schoof: Proposition 8.2)*

Seien p, q verschiedene, ungerade Primzahlen. Erfüllen $x, y \in \mathbb{Z} - \{0\}$ die Gleichung $x^p - y^q = 1$ und ist $(x - \zeta_p)^{1-\iota} = \alpha^q$ für ein $\alpha \in \mathbb{Q}^*(\zeta_p)$, dann gilt:

$$q \equiv 1 mod\ p$$

Hat man dieses Resultat, dass $q \equiv 1 (\text{mod } p)$, sind in $\mathbb{Q}_p(\zeta_p)$ keine nicht-trivialen q-ten Einheitswurzeln enthalten und die obige Darstellung von w' ergibt sich quasi von selbst.

3.3 Normberechnung im p-adischen

Wir haben nun alles beisammen, um den entscheidenden Satz zu beweisen.

Satz 3.2. *(vgl. Schoof: Theorem 8.3)*

Seien p, q verschiedene, ungerade Primzahlen und mögen $x, y \in \mathbb{Z} - \{0\}$ die Gleichung $x^p - y^q = 1$ erfüllen.

Dann ist $(x - \zeta_p)^{1-\iota} \in H^-$ nicht trivial.

Beweis. Angenommen, $(x - \zeta_p)^{1-\iota}$ sei trivial. Dann lassen sich mittels $\alpha \in \mathbb{Q}(\zeta_p)$, für das $(x - \zeta_p)^{1-\iota} = \alpha^q$ gilt, die q-ten Wurzeln $w, w' = \frac{w}{\alpha}$ wie zuvor beschrieben als p-adische Reihe konstruieren. Wir betrachten in $\mathbb{Q}_p(\zeta_p)$ das Element $u = w - w'$, dessen q-te Potenz unsere Einheit η ergibt, und berechnen $N(\eta) = N(u)^q$.

Für die Rechnung setzen wir wieder $\mu := \frac{x-1}{1-\zeta_p}$, so dass wir $w^q = \frac{x-\zeta_p}{1-\zeta_p} = 1 + \mu$, $w'^q = -\zeta_p^{-1} \cdot (1 + \overline{\mu})$ haben (vgl. Abschnitt 3.2) und

$$\overline{\mu} = \frac{x-1}{1-\overline{\zeta_p}} = -\zeta_p \cdot \frac{x-1}{1-\zeta_p} = -\zeta_p \cdot \mu.$$

Rechne nun mod μ^3 in $\mathbb{Z}_p[\zeta_p]$:

$$\begin{aligned}
u = w - w' &= \sqrt[q]{1+\mu} + \zeta_p^r \sqrt[q]{1+\overline{\mu}} \\
&\equiv 1 + \frac{1}{q}\mu + \binom{\frac{1}{q}}{2}\mu^2 + \zeta_p^{-1}\left(1 + \frac{1}{q}\overline{\mu} + \binom{\frac{1}{q}}{2}\overline{\mu}^2\right) && | r \equiv rq \equiv -1\ (p), \text{Prop. 3.1} \\
&\equiv (1 + \zeta_p^{-1}) + \binom{\frac{1}{q}}{2}\mu^2(1 + \zeta_p^{-1})\zeta_p && | \overline{\mu} = -\zeta_p \cdot \mu \\
&\equiv (1 + \zeta_p^{-1})\left(1 + \frac{1-q}{2q^2}(x-1)^2\frac{\zeta_p}{(1-\zeta_p)^2}\right)
\end{aligned}$$

Die Zahl in der linken Klammer ist nach Lemma 2.1 eine Einheit und fällt daher bei der Normbildung weg. Weiterhin ist das Ideal $\mu^3\mathbb{Z}_p[\zeta_p]$ für alle p-ten Einheitswurzeln $\zeta \in \mu_p, \zeta \neq 1$ gleich, weil $(1 - \zeta_p) = \epsilon \cdot (1 - \zeta_p^s)$ mit $\epsilon \in \mathbb{Z}_p[\zeta_p]^*$ für $1 \leq s < p$.

Also erhalten wir:

$$\begin{aligned}
N(u) &= \prod_{\zeta \in \mu_p, \zeta \neq 1}\left(1 + \frac{1-q}{2q^2}(x-1)^2\frac{\zeta}{(1-\zeta)^2}\right) (\text{mod } \mu^3) \\
&= 1 + \frac{1-q}{2q^2}(x-1)^2 \cdot \sum_{\zeta \in \mu_p, \zeta \neq 1}\frac{\zeta}{(1-\zeta)^2}
\end{aligned}$$

Mit der ein wenig überraschenden Identität $\sum_{\zeta\in\mu_p,\zeta\neq 1}\frac{\zeta}{(1-\zeta)^2}=\frac{1-p^2}{12}$, die im Anhang bewiesen wird, erhalten wir

$$N(\eta)=N(u)^q\equiv 1+\frac{1-q}{2q}(x-1)^2\frac{1-p^2}{12}(\text{mod }\mu^3)$$

denn wir haben neben der 1 nur q gleiche Terme, die nicht modulo μ^3 „verschwinden“.

Da $N(\eta)=1$ gilt, folgt notwendigerweise die Teilbarkeit

$$\mu^3=\frac{(x-1)^3}{(1-\zeta_p)^3}=-\frac{(x-1)^3}{\pi^3}\text{ teilt }\frac{1-q}{2q}(x-1)^2\frac{1-p^2}{12}.$$

Das bedeutet, dass $x-1\mid\frac{1-q}{2q}\frac{1-p^2}{12}\cdot\pi^3$ in $\mathbb{Z}_p[\zeta_p]$.

Nach Cassels haben wir $x-1\equiv 0 \bmod p^{q-1}$ und $1-p^2\equiv 0 \bmod 4$, weil p ungerade. Somit muss $p^{q-1}|(1-q)\frac{\pi^3}{3}$ gelten.

Wir beobachten, dass $\frac{\pi^3}{3}\mid p$, denn für $p=3$ gilt $\frac{\pi^3}{3}=\frac{3\epsilon\cdot\pi}{3}=\epsilon\cdot\pi$ für eine Einheit ϵ und ansonsten ist bereits $\frac{1}{3}$ eine Einheit.

Das führt uns zu $p^{q-1}\mid(1-q)\cdot p$ und $p^{q-2}\mid 1-q$. Gleichzeitig gilt aber sicherlich $p^{q-2}>q-1$.

Widerspruch, die Teilbarkeit kann nicht erfüllt sein, also kann $(x-\zeta_p)^{1+\iota}$ doch nicht trivial sein.

□

4 Untere Schranke für p und q

Mit den bisherigen Ergebnissen lassen sich nun leicht die folgenden Resultate formulieren.

Korollar 4.1. *Seien p,q verschiedene, ungerade Primzahlen. Wenn $q\nmid h_p^-$ oder $p\nmid h_q^-$, hat die Gleichung $x^p-y^q=1$ keine Lösung $x,y\in\mathbb{Z}-\{0\}$.*

Beweis. Aus Symmetriegründen betrachten wir nur den Fall $q\nmid h_p^-$. Dann ist $Cl_p^-[q]$ trivial. Weil $Cl_p^-[q]\cong H^-$, kann es keine Lösung geben, da sonst H^- nicht trivial wäre. □

Durch einen kurzen Blick in einschlägige Klassenzahltafeln erhält man hiermit den abschließenden

Satz 4.2. *Seien p,q verschiedene, ungerade Primzahlen und p oder $q\leq 41$. Dann hat die Gleichung $x^p-y^q=1$ keine Lösung $x,y\in\mathbb{Z}-\{0\}$.*

Literatur

[Schoof] Schoof, René. *„Catalan's Conjecture“*. Springer-Verlag, New York, 2009

[LWash] Washington, Lawrence C. *„Introduction to Cyclotomic Fields“*. Graduate Texts in Mathematics, Vol. 83 Springer-Verlag, New York, 1997

[Neukirch] Neukirch, Jürgen. *„Algebraische Zahlentheorie“*, Kapitel II. Springer-Verlag, New York, 2006

Anhang

In Anlehnung an [Schoof], Exercise 8.4 beweisen wir das folgende

Lemma 4.3. *Sei $n \in \mathbb{N}$ und bezeichne μ_n die Gruppe der komplexen n-ten Einheitswurzeln.*

Es gilt die Identität: $\sum_{1 \neq \zeta \in \mu_n} \frac{\zeta}{(1-\zeta)^2} = \frac{1-n^2}{12}$

Beweis. Für $k \geq 1$ setze $s_k = \sum_{\zeta \in \mu_n, \zeta \neq 1} \frac{1}{(1-\zeta)^k}$.

Man hat dann

$$s_2 - s_1 = \sum_{\zeta \in \mu_n, \zeta \neq 1} \frac{1}{(1-\zeta)^2} - \sum_{\zeta \in \mu_n, \zeta \neq 1} \frac{1}{1-\zeta} = \sum_{\zeta \in \mu_n, \zeta \neq 1} \frac{1-(1-\zeta)}{(1-\zeta)^2} = \sum_{\zeta \in \mu_n, \zeta \neq 1} \frac{\zeta}{(1-\zeta)^2}$$

.

Wir berechnen s_2 und s_1 mithilfe der Potenzreihenentwicklung des Logarithmus $log(1+X) = \sum_{k \geq 1} (-1)^{k-1} \frac{X^k}{k}$ und der Polynomgleichung $(*)$ $\prod_{\zeta \in \mu_n, \zeta \neq 1} X - \zeta = \frac{X^n - 1}{X - 1}$.

$$\begin{aligned}
\sum_{k \geq 1} s_k \frac{X^k}{k} &= \sum_{\zeta \in \mu_n, \zeta \neq 1} \sum_{k \geq 1} \frac{(\frac{X}{1-\zeta})^k}{k} \\
&= \sum_{\zeta \in \mu_n, \zeta \neq 1} -log\left(1 - \frac{X}{1-\zeta}\right) \\
&= -log\left(\prod_{\zeta \in \mu_n, \zeta \neq 1} \left(1 - \frac{X}{1-\zeta}\right)\right) \\
&= -log\left(\prod_{\zeta \in \mu_n, \zeta \neq 1} \frac{(1-X)-\zeta}{1-\zeta}\right) \\
&= -log\left(\prod_{\zeta \in \mu_n, \zeta \neq 1} \frac{Y-\zeta}{1-\zeta}\right) && |Y = 1 - X \\
&= -log\left(\frac{Y^n - 1}{n \cdot (Y-1)}\right) && |(*), \prod_{\zeta \neq 1} 1 - \zeta = n \\
&= -log\left(\frac{((1-X)^n - 1}{-nX}\right) \\
&= -log\left(1 + \frac{\binom{n}{2}X^2 - \binom{n}{3}X^3 \ldots \pm X^n}{-nX}\right) \\
&= \frac{(n-1)}{2}X - \frac{(n-1)(n-2)}{6}X^2 + \frac{(n-1)^2}{8}X^2 + O(X^3) \\
&= \frac{(n-1)}{2}\frac{X}{1} - \frac{(n-1)(n-5)}{12}\frac{X^2}{2} + O(X^3)
\end{aligned}$$

Einsetzen liefert das gewünschte Resultat:

$$\sum_{\zeta \in \mu_n, \zeta \neq 1} \frac{\zeta}{(1-\zeta)^2} = s_2 - s_1 = -\frac{(n-1)(n+1)}{12} = \frac{1-n^2}{12}$$

.

□