Über den zweiten Faktor der Klassenzahl und den Irregularitätsgrad der irregulären Kreiskörper.

Dem Andenken des unvergesslichen Freundes, Prof. Tibor Szele gewidmet.

Von PETER DÉNES in Budapest.

Es bezeichne p eine irreguläre Primzahl, ζ eine primitive p-te Einheitswurzel, $R(\zeta)$ den Kreiskörper der p-ten Einheitswurzeln, $\lambda=1-\zeta$, $\mathfrak{l}=(\lambda)$. Bekanntlich ist $\mathfrak{l}^{p-1}=(p)$.

Der zweite Faktor der Klassenzahl des Kreiskörpers $R(\zeta)$ ist:

$$h_2=\frac{\Delta}{R}, \tag{1}$$

wo Δ die Determinante

$$\Delta=\left|\log \varepsilon^{s^{i+k}}\right| \qquad \left(k=0,1,\ldots,\frac{p-5}{2}\right) \quad \left(i=0,1,\ldots,\frac{p-5}{2}\right) \tag{2}$$

repräsentiert, in welcher

$$\varepsilon=\sqrt{\frac{(1-\zeta^r)(1-\zeta^{-r})}{(1-\zeta)(1-\zeta^{-1})}} \tag{3}$$

ist und die symbolische Potenz s^g die Substitution $\zeta\to\zeta^{r^g}$ bezeichnet, wobei r eine primitive Wurzel modulo p ist; ferner ist R der Regulator des Körpers $R(\zeta)$, also die Determinante eines Systems von Fundamentaleinheiten $\varrho_1,\ldots,\varrho_{\frac{p-3}{2}}$:

$$R=\left|\log \varrho_k^{s^i}\right| \qquad \left(\mathrm{k}=1,2,\ldots,\frac{p-3}{2}\right) \quad \left(i=0,1,\ldots,\frac{p-5}{2}\right). \tag{4}$$

Wir nehmen an, daß h_2, der zweite Faktor der Klassenzahl des Körpers $R(\zeta)$ genau durch die f_2-te Potenz von p teilbar ist:

$$h_2=p^{f_2}\cdot q, \tag{5}$$

wobei q eine zu p prime ganze Zahl bezeichnet.

VANDIVER [6] zeigte, daß eine notwendige und hinreichende Bedingung für p/h_2 ist, daß eine der Einheiten E_i

$$E_i = \varepsilon^{G_i} \qquad \left(i=1,\ldots,\frac{p-3}{2}\right),$$

wobei G_i eine symbolische Potenz

$$G_i = r^{p^2} + s r^{p^2-2i} + s^2 r^{p^2-4i} + \cdots + s^{\frac{p-3}{2}} r^{-(p-3)i}$$

bedeutet, die p-te Potenz einer Einheit in $R(\zeta)$ ist. Wir wollen den Wert f_2 in (5) in der vorliegenden Arbeit genau feststellen.

Satz 1. *Ist die primitive Wurzel r modulo p in der Weise gewählt, daß die Kongruenz*

$$r^{p-1} \equiv 1 \pmod{p^F}, \tag{6}$$

$F > f_2 + 1$ erfüllt wird und werden die Einheiten E_i

$$E_i = \varepsilon^{S_i} \qquad \left(i=1,\ldots,\frac{p-3}{2}\right), \tag{7}$$

durch die symbolischen Potenzen

$$S_i = 1 + s r^{-2i} + s^2 r^{-4i} \ldots + s^{\frac{p-3}{2}} r^{-(p-3)i} \tag{8}$$

erzeugt und sind schließlich die Einheiten E_i im allgemeinen p^{ν_i}-te Potenzen von Einheiten aus $R(\zeta)$:

$$E_i = \delta_i^{p^{\nu_i}} \qquad \left(i=1,\ldots,\frac{p-3}{2}\right), \tag{9}$$

$\delta_i \in R(\zeta)$, so ist

$$f_2 = \sum_{i=1}^{\frac{p-3}{2}} \nu_i. \tag{10}$$

BEWEIS. Im Körper $R(\zeta)$ gibt es nach POLLACZEK [4] ein System von fundamentalen Einheiten $\varrho_1,\ldots,\varrho_{\frac{p-3}{2}}$, für welche die folgenden Gleichungen bestehen:

$$\varrho_i^{s-r^{2i}p^{c-1}} = H_i^{p^c} \qquad \left(i=1,\ldots,\frac{p-3}{2}\right), \tag{11}$$

wobei c eine beliebige ganze rationale Zahl ist und $H_1,\ldots,H_{\frac{p-3}{2}}$ Einheiten in $R(\zeta)$ sind. Wir wählen

$$c > f_2, \text{ jedoch } F > c. \tag{12}$$

Die Kreiseinheit ε kann vermittelst der fundamentalen Einheiten in (11) ausgedrückt werden;

$$\varepsilon = \sum_{k=1}^{\frac{p-3}{2}} \varrho_k^{a_k}; \tag{13}$$

hier bezeichnen $a_1, \ldots, a_{\frac{p-3}{2}}$ ganze rationale Zahlen. Wenden wir auf (13) die Substitution s^i an, so erhalten wir zufolge (11) eine Gleichung

$$\varepsilon^{s^i} = \prod_{k=1}^{\frac{p-3}{2}} \varrho_k^{a_k \cdot r^{2ikp^{c-1}}} H_i'^{p^c} \qquad \left(i = 1, 2, \ldots, \frac{p-5}{2}\right), \tag{14}$$

in welcher $H_1', \ldots, H'_{\frac{p-5}{2}}$ Einheiten aus $R(\zeta)$ sind. Aus (13) und (14) ergeben sich ferner

$$\log \varepsilon^{s^i} = \sum_{k=1}^{\frac{p-3}{2}} a_k r^{2ikp^{c-1}} \cdot \log \varrho_k + p^c \log H_i' \quad \left(i = 0, 1, \ldots, \frac{p-5}{2}\right). \tag{15}$$

Gemäß dem Multiplikationsregel der Determinanten erhalten wir aus (1), (2), (4) und (15) die Kongruenz

$$h_2 \equiv \left| a_k \cdot r^{2ikp^{c-1}} \right| \quad \begin{pmatrix} i = 0, 1, \ldots, \frac{p-5}{2} \\ k = 1, 2, \ldots, \frac{p-3}{2} \end{pmatrix} \pmod{p^c}, \tag{16}$$

welche nach der VANDERMONDE'schen Lösung

$$h_2 \equiv \prod_{k=1}^{\frac{p-3}{2}} a_k \prod_{i, j=0, j<i}^{\frac{p-3}{2}} \left(r^{2ip^{c-1}} - r^{2jp^{c-1}}\right) \pmod{p^c} \tag{17}$$

ergibt. Da für $2i \not\equiv 2j \pmod{p-1}$ $r^{2ip^{c-1}} \not\equiv r^{2jp^{c-1}} \pmod{p}$ gilt, folgt aus (17)

$$\prod_{k=1}^{\frac{p-3}{2}} a_k \equiv 0 \pmod{p^{f_2}}, \tag{18}$$

jedoch

$$\prod_{k=1}^{\frac{p-3}{2}} a_k \not\equiv 0 \pmod{p^{f_2+1}}. \tag{19}$$

Die Gleichungen (7) lassen sich mit Hilfe von (13) und (14) folgenderweise umformen:

$$E_i = \prod_{k=1}^{\frac{p-3}{2}} \varrho_k^{a_k \sum_{j=0}^{\frac{p-3}{2}} r^{2jkp^{c-1} - 2ij}} \cdot H_i''^{p^c} \quad \left(i = 1, \ldots, \frac{p-3}{2}\right), \tag{20}$$

wobei $H_1'', \ldots, H''_{\frac{p-3}{2}}$ Einheiten in $R(\zeta)$ bezeichnen. Die Summe an der rechten Seite der Gleichung (20) ist

$$\sum_{j=0}^{\frac{p-3}{2}} r^{2jkp^{c-1} - 2ij} = \frac{r^{(p-1)(kp^{c-1} - i)} - 1}{r^{2kp^{c-1} - 2i} - 1}. \tag{21}$$

Falls $i \neq k$, $r^{2kp^{c-1}-2i} \not\equiv 1 \pmod{p}$, folglich wegen (6) und (12)

$$\sum_{j=0}^{\frac{p-3}{2}} r^{2jkp^{c-1}-2ij} \equiv 0 \pmod{p^c};$$

im Gegenteil, wenn $k=i$ ist, ist zufolge (12)

$$\sum_{j=0}^{\frac{p-3}{2}} r^{2jkp^{c-1}-2ij} \equiv \frac{p-1}{2} \pmod{p^c}.$$

Hieraus folgt die einfache Form von (20):

$$E_i = \varrho_i^{a_i \cdot \frac{p-1}{2}} \cdot H_i'''^{p^c} \quad \left(i=l,\ldots,\frac{p-3}{2}\right), \tag{22}$$

in welcher $H_1''', \ldots, H_{\frac{p-3}{2}}'''$ Einheiten in $R(\zeta)$ bezeichnen.

Aus (22) können wir — mit Rücksicht auf (12) — folgern, daß die Einheit E_i dann und nur dann die p^{v_i}-te Potenz einer Einheit in $R(\zeta)$ ist, wenn p^{v_i}/a_i besteht. (18) und (19) ergeben mit diesem Resultat den vollständigen Beweis des Satzes.

Der Wert des Exponenten f_2 kann mittels spezieller Zahlenreihen, welche den irregulären Kreiskörper charakterisieren, bestimmt werden. Diese Zahlenreihen wurden in früheren Arbeiten folgenderweise definiert:

Das „p-Charakter der Bernoullischen Zahlen" [1], $u_1, \ldots, u_{\frac{p-3}{2}}$, werden gemäß der folgenden Kongruenzen, bzw. Inkongruenzen festgelegt:

$$B_{ip^j} \equiv 0 \pmod{p^{2j+1}} \quad \left(i=1,\ldots,\frac{p-3}{2}\right), \quad (j=0,\ldots,u_i-1), \tag{23}$$

$$B_{ip^{u_i}} \not\equiv 0 \pmod{p^{2u_i+1}} \quad \left(i=1,\ldots,\frac{p-3}{2}\right). \tag{24}$$

Das „p-Charakter der Kreiskörpergrundeinheiten" [2], $u_1', \ldots, u_{\frac{p-3}{2}}'$, kommen in dem Grundeinheitssystem von $R(\zeta)$ in folgender Form vor:

$$\varrho_i \equiv m_i + n_i \lambda^{u_i'(p-1)+2i} \pmod{\mathfrak{l}^{u_i'(p-1)+2i+1}} \quad \left(i=1,\ldots,\frac{p-3}{2}\right), \tag{25}$$

wobei $m_1, \ldots, m_{\frac{p-3}{2}}, n_1, \ldots, n_{\frac{p-3}{2}}$ ganze rationale, zu p prime Zahlen sind.

Der Exponent von p, mit welcher der zweite Faktor der Klassenzahl von $R(\zeta)$ teilbar ist, kann mit Hilfe dieser Zahlenreihen folgenderweise ermittelt werden:

Satz 2. *Bezeichnet f_2 das Exponent von p, mit welchem h_2, der zweite Faktor der Klassenzahl von $R(\zeta)$ teilbar ist, so gilt*

$$f_2 = \sum_{i=1}^{\frac{p-3}{2}} (u_i - u_i'), \tag{26}$$

wo $u_1 = u_{\frac{p-3}{2}}$ das p-Charakter der Bernoullischen Zahlen und $u_1', \ldots, u_{\frac{p-3}{2}}'$ das p-Charakter der Kreiskörpergrundeinheiten sind.

Beweis. Erfüllt die Zahl F nicht nur die Bedingung in (6): $F > f_2$, sondern auch $F > w$, wobei w den Irregularitätsgrad der Primzal p bezeichnet [1], so sind die Einheiten E_i in (7) dieser Arbeit mit den Einheiten β_j $\left(j = 1, \ldots, \frac{p-3}{2}\right)$ in ([1], Satz 1) ersetzbar, wobei für i und j der Zusammenhang

$$i = \frac{p-1}{2} - j$$

gilt. Darüber kann mann sich durch das Vollziehen der gezeichneten Operationen sofort überzeugen:

$$\beta_j = \prod_{k=1}^{\frac{p-1}{2}} \varepsilon_k^{r^{2kj}} \qquad \left(j = 1, \ldots, \frac{p-3}{2}\right) \tag{27}$$

und hier steht ε_k für $\varepsilon_k = \varepsilon^{s^k}$, gemäß der, in dieser Arbeit angewendeten Bezeichnungsart. (27) kann daher auch vermittelst symbolischer Potenz ausgedrückt werden:

$$\beta_j = \varepsilon^{S_i'}, \qquad \left(i = 1, \ldots, \frac{p-3}{2}\right) \tag{28}$$

wo

$$S_i' = s r^{p-1-2i} + s^2 r^{2(p-1)-4i} + \cdots + s^{\frac{p-1}{2}} r^{\frac{p-1}{2}(p-1)-(p-1)i} \qquad \left(i = 1, \ldots, \frac{p-3}{2}\right) \tag{29}$$

ist. Mit Anbetracht auf (6) und auf $\varepsilon^{s^{\frac{p-1}{2}}} = \varepsilon$ folgt aus (8) und (29):

$$\varepsilon^{S_i} = \varepsilon^{S_i} \vartheta_i^{p^{w+1}} \tag{30}$$

mit einer Einheit ϑ_i aus $R(\zeta)$. Da die p^{w+1}-te Potenz einer Zahl aus $R(\zeta)$ mit einer ganzen rationalen Zahl modulo p^{w+1} kongruent ist, folgt die Kongruenz aus (30) und aus ([1], Relation (10)):

$$E_i \equiv A_i + B_i \lambda^{(p-1)u_i+2i} \pmod{\mathfrak{l}^{(p-1)u_i+2i+1}} \quad \left(i = 1, \ldots, \frac{p-3}{2}\right), \tag{31}$$

wobei $A_1, \ldots, A_{\frac{p-3}{2}}, B_1, \ldots, B_{\frac{p-3}{2}}$ ganze rationale, zu p prime Zahlen sind.

Wählt man nun die Zahl c in (12) auf die Weise, daß sie außer (12) auch der Bedingung $c > w$ genüge, so ist $H_i'''^{p^c}$ in (22) mit einer ganzen rationalen Zahl g_i modulo p^{w+1} kongruent und damit folgt aus (22) die Kongruenz:

$$(32) \qquad E_i \equiv g_i \varrho_i^{y_i p^{v_i}} \pmod{\mathfrak{l}^{(p-1)w+1}} \quad \left(i = 1, \ldots, \frac{p-3}{2}\right),$$

wobei y_i eine zu p prime Zahl bezeichnet. Aus (25) und (31) ergibt also (32) wegen $\mathfrak{l}^{p-1} = (p)$ sofort:

$$(33) \qquad v_i = u_i - u_i' \qquad \left(i = 1, \ldots, \frac{p-3}{2}\right),$$

woraus wegen (10) der vollständige Beweis des Satzes folgt.

In der früheren Arbeit [1] habe ich das Problem aufgeworfen, ob der Irregularitätsgrad w des Kreiskörpers $R(\zeta)$ für eine endliche Primzahl p endlich sein muß? Zwar verwahrscheinlicht die Gleichung (26) — wo f_2 unbedingt endlich ist — diese Vermutung, zu dem präzisen Beweis dieser Tatsache sind noch einige, in späteren Arbeiten zu veröffentlichenden Eigenschaften des Kreiskörpers notwendig.

Nun wollen wir die Endlichkeit von w für endliche p unter Voraussetzung der Richtigkeit der Klassenkörperturmvermutung in einfacher Weise bestätigen.

Der Klassenkörperturm wird zu einem endlichen algebraischen Zahlkörper k folgenderweise aufgestellt: K_1 bezeichne den Klassenkörper von k, K_2 den Klassenkörper von K_1, und so weiter, im allgemeinen K_{i+1} bezeichnet den Klassenkörper von K_i. So kann man die Reihe $k, K_1, \ldots, K_n, \ldots$ aufstellen.

Gemäß der berühmten Vermutung von FURTWÄNGLER soll diese Reihe von Klassenkörpern bei einer endlichen Zahl n abbrechen, d.h. die Klassenzahl von K_n ist gleich Eins und K_n ist mit seinem Klassenkörper identisch. (Erörterungen für spezielle Fälle siehe z.B. [5]).

Unter den Zahlen $u_1', \ldots, u_{\frac{p-3}{2}}'$ sei etwa $u_t' = w'$ die größte, wo w' der reduzierte Irregularitätsgrad von $R(\zeta)$ genannt wurde ([2], § 3, S. 203.) Für die Einheit ϱ_t in (25) gilt dann die Kongruenz

$$(34) \qquad \varrho_t \equiv m_t \pmod{\mathfrak{l}p^{w'}}$$

wobei m_t eine ganze rationale, zu p prime Zahl ist. Da es ferner aus (27), (32), (33) und ([1], Relation (10)) folgt, daß

$$(35) \qquad E_t^{p-1} \equiv 1 \;(\mathrm{mol}\; \mathfrak{l}p^{w'+v_t})$$

ist, bekommen wir aus (32):

$$(36) \qquad g_t^{p-1} \varrho_t^{y_t p^{v_t} p-1} \equiv 1 \pmod{\mathfrak{l}p^{w'+v_t}}.$$

Nun ist wegen $c > w$ die Einheit $H_t'''^{p^c}$ mit der p^{w+1}-ten Potenz einer ganzen rationalen Zahl modulo p^{w+1} kongruent, bezeichnet durch g_t. Hieraus folgt, daß

$$g_t^{p-1} \equiv 1 \qquad (\mathrm{mod}\ p^{w+1})$$

ist und da gemäß den Definitionen $w \geqq w' + \nu_t$ gilt, ergibt sich hiemit aus (36):

$$\delta_t = \varrho_t^{y_t(p-1)} \equiv 1 \qquad (\mathrm{mod}\ \mathfrak{l}p^{w'}); \tag{37}$$

jedoch ist die Kongruenz (37) für den Modul $\mathfrak{l}p^{w'+1}$ nicht mehr gültig.

Ist $w' > 0$, so ist δ_t eine singuläre Primärzahl in $R(\zeta)$ [3] und die Adjunktion der p-ten Wurzel von δ_t erzeugt einen Teilklassenkörper über $R(\zeta)$. Die Zahl

$$\sqrt[p]{\delta_t}$$

liegt also in K_1, im ersten absoluten Klassenkörper von $R(\zeta)$. Wir nehmen an, daß nicht nur $\sqrt[p]{\delta_t}$, sondern auch die Zahl Π_1

$$\Pi_1 = \sqrt[p^{z_1}]{\delta_t}$$

in K_1 liegt; die p-te Wurzel von Π_1 ist jedoch keine Zahl in K_1. Aus der Unverzweigtheit von K_1 über $R(\zeta)$ folgt, daß eine Kongrunez

$$\delta_t \equiv 1 \ (\mathrm{mod}\ \mathfrak{l}p^{z_1}) \tag{38}$$

bestehen muß; ferner muß z_1 eine endliche Zahl sein, weil der absolute Grad des Körpers K_1 endlich ist und der Grad der algebraischen Gleichung, welcher Π_1 genügt, wenigstens p^{z_1} ist, den Grad von K_1 jedoch nicht überschreiten kann. Aus (37) und (38) gilt ferner

$$w' \geqq z_1. \tag{39}$$

Gilt in (39) $w' > z_1$, so ist die Zahl Π_1 eine singuläre Primärzahl in K_1 und bestimmt ihre p-te Wurzel einen Teilklassenkörper von K_1. Wir nehmen wieder an, daß außer $\sqrt[p]{\Pi_1}$ auch die Zahl

$$\Pi_2 = \sqrt[p^{z_2}]{\Pi_1}$$

in K_2 liegt, die Zahl $\sqrt[p]{\Pi_2}$ jedoch nicht. Hier bezeichnet K_2 den absoluten Klassenkörper von K_1. Wie vorher, können wir für die Zahl z_2 die Zusammenhänge

$$\delta_t \equiv 1 \ (\mathrm{mod}\ \mathfrak{l}p^{z_1+z_2})$$

und

$$w' \geqq z_1 + z_2 \tag{40}$$

folgern, wie auch die Tatsache, daß z_2 endlich sein muß. Gilt in (40) das Ungleichungszeichen, so können wir auf gleiche Weise fortfahren. Da die Anzahl der Reihe von Klassenkörpern bei n abbricht, kann K_n keine singuläre Primärzahl enthalten. Die entsprechende Relation von (40) für K_n ist also nur für das Gleichheitszeichen gültig:

$$w' = z_1 + z_2 + \cdots + z_n. \tag{41}$$

Die Zahlen $z_1, \ldots, z_n$ und n sind sämtlich endliche Zahlen; demzufolge ist auch w' endlich. Da aber w' die größte unter den Zahlen $u'_1, \ldots, u'_{\frac{p-3}{2}}$ bezeichnet, sind sowohl diese Zahlen, wie auch ihre Summe endlich. Ferner ist auch die Klassenzahl von $R(\zeta)$ und daher auch f_2 endlich. Aus (26) folgt daher, daß auch

$$\sum_{i=1}^{\frac{p-3}{2}} u_i.$$

also sämtliche Mitglieder der Zahlenreihe $u_1, \ldots, u_{\frac{p-3}{2}}$ endlich sind. Hiedurch ist bewiesen, daß w — die größte in dieser Zahlenreihe — selbst endlich sein muß.

Literatur.

[1] P. Dénes, Über irreguläre Kreiskörper, *Publ. Math. Debrecen* **3** (1953), 17—23.

[2] P. Dénes, Über Grundeinheitssysteme der irregulären Kreiskörper von besonderen Kongruenzeigenschaften, *Publ. Math. Debrecen* **3** (1954), 195—204.

[3] Ph. Furtwängler, Allgemeiner Existenzbeweis für den Klassenkörper eines beliebigen algebraischen Zahlkörpers, *Math. Ann.* **63** (1906), 1—37.

[4] F. Pollaczek, Über die irregulären Kreiskörper der l-ten und l^2-ten Einheitswurzeln, *Math. Z.* **21** (1924), 1—38.

[5] A. Scholz, Zwei Bemerkungen zum Klassenkörperturm, *J. Reine Angew. Math.* **161** (1929), 201—207.

[6] H. S. Vandiver, On the second factor of the class number of a cyclotomic field, *Proc. Nat. Acad. Sci. U.S.A.* **16** (1930), 743—749.

(Eingegangen am 8. August, 1955.)