Über irreguläre Kreiskörper.

Von PETER DÉNES in Budapest.

Wir bezeichnen mit p eine irreguläre Primzahl, r eine primitive Wurzel modulo p, $q = \frac{p-3}{2}$, $\zeta = e^{2\pi i/p}$, $\Omega(\zeta)$ den zu p gehörigen Kreiskörper, $\lambda = 1-\zeta$, $\mathfrak{l} = (\lambda)$.

Wenn p eine irreguläre Primzahl ist, sind die ersten q Bernoullischen Zahlen nicht sämtlich prim zu p[1]). Es soll unter den Zahlen $B_1, \ldots, B_q$ die Zähler von g Zahlen: $B_{m_1}, B_{m_2}, \ldots, B_{m_g}$ durch p teilbar sein. Ferner sollen die folgenden Kongruenzen bestehen:

$$B_{ip^j} \equiv 0 \pmod{p^{2j+1}} \qquad (j = 0, 1, \ldots, u_i - 1), \tag{1a}$$

jedoch

$$B_{ip^{u_i}} \not\equiv 0 \pmod{p^{2u_i+1}} \qquad (i = m_1, \ldots, m_g) \tag{1b}$$

sein, wodurch zu jeder Zahl $m_1, m_2, \ldots, m_g$ eine eindeutig bestimmte Zahl $u_{m_1}, \ldots, u_{m_g}$ zugeordnet wird. Ist B_i $(i \leqq q)$ prim zu p, so ist $u_i = 0$.

Die Zahlen $u_1, \ldots, u_q$ sollen das „p-Charakter der Bernoullischen Zahlen" heißen, und die größte unter denselben, bezeichnet durch w, heiße der Irregularitätsgrad des Körpers $\Omega(\zeta)$, bzw. der Irregularitätsgrad der Primzahl p. Ist p regulär, so ist w gleich Null.

Nun wirft sich die Frage auf, ob es zu einer jeden Bernoullischen Zahl B_{m_j} ein endlicher Wert von u_{m_j} gehört, mit welcher die Inkongruenz in (1b) erfüllt wird, bzw., mit anderen Worten, ob der Irregularitätsgrad einer Primzahl notwendigerweise endlich ist? Die Frage kann bejahend beantwortet werden, und einen Beweis hiefür werden wir in einer späteren Arbeit mitteilen.

Wir nehmen also an, daß der Irregularitätsgrad von p endlich ist und bestimmen analoge Gesetze für die irregulären Kreiskörpereinheiten zu denjenigen, welche KUMMER im regulären Kreiskörper gewonnen hat. Diese Gesetze erlauben einen Einblick in den konstruktionellen Unterschied der regulären und irregulären Kreiskörper.

---

[1]) D. HILBERT, Bericht über die Theorie der algebraischen Zahlkörper, Berlin, 1897. Satz 154.

Satz 1. *Ist p eine ungerade Primzahl, so gibt es in dem, zu p gehörigen Kreiskörper $\Omega(\zeta)$ ein unabhängiges Einheitssystem, welches die Kongruenzen*

$$\eta_i \equiv 1 + \lambda^{2e_i} \pmod{\mathfrak{l}^{2e_i+1}} \qquad (i = 1, \ldots, q) \tag{2}$$

erfüllt, wo $2e_i = u_i(p-1)+2i$ gilt, und $u_1, \ldots, u_q$ das p-Charakter der Bernoullischen Zahlen bezeichnen.

Beweis. Die sogenannten Kreiseinheiten werden durch die Formel definiert:

$$\varepsilon_k = \sqrt{\frac{(\zeta^{r^{k+1}}-1)(\zeta^{-r^{k+1}}-1)}{(\zeta^{r^k}-1)(\zeta^{-r^k}-1)}} \qquad \left(k = 1, 2, \ldots, \frac{p-1}{2}\right). \tag{3}$$

Wir bestimmen ferner die Einheiten $\beta_1, \ldots, \beta_q$ durch die Relationen

$$\beta_j = \prod_{k=1}^{\frac{p-1}{2}} \varepsilon_k^{r^{2kj}} \qquad (j = 1, \ldots, q),$$

beziehungsweise, mit Rücksicht auf $\varepsilon_1 \ldots \varepsilon_{\frac{p-1}{2}} = 1$, durch

$$\beta_j = \prod_{k=1}^{q} \varepsilon_k^{r^{2kj} - r^{(p-1)j}} \qquad (j = 1, \ldots, q). \tag{4}$$

Zunächst bestätigen wir, daß diese Einheiten bei jedem gewählten Wert der Primitivzahl r ein unabhängiges Einheitssystem darstellen. Es genügt zu zeigen, daß es keine rationale, nicht sämtlich verschwindende Zahlen $n_1, \ldots, n_q$ gibt, mit welchen eine Gleichung

$$\prod_{j=1}^{q} \beta_j^{n_j} = 1$$

besteht[2]), d. h. daß die Determinante

$$D(\beta_1, \ldots, \beta_q) = |\log \beta_j^{(g)}| \qquad \begin{matrix}(j = 1, \ldots, q)\\ (g = 1, \ldots, q)\end{matrix}$$

nicht verschwindet, wobei $\beta_j^{(g)}$ diejenige Einheit bezeichnet, welche aus β_j durch die Substitution $\zeta^r \to \zeta^{r^g}$ entspringt. Aus (4) und aus den konjugierten Gleichungen von (4) folgt

$$\log \beta_j^{(g)} = \sum_{k=1}^{q} (r^{2kj} - r^{(p-1)j}) \cdot \log \varepsilon_k^{(g)} \qquad \begin{matrix}(j = 1, \ldots, q)\\ (g = 1, \ldots, q).\end{matrix}$$

Bezeichnet man durch Δ die Determinante der Kreiseinheiten:

$$\Delta = |\log \varepsilon_k^{(g)}| \qquad (g = 1, \ldots, q;\ k = 1, \ldots, q),$$

(wo $\Delta \neq 0$ gilt, da die Kreiseinheiten ein unabhängiges Einheitssystem bilden), und setzt man ferner

$$D_1 = \frac{D(\beta_1, \ldots, \beta_q)}{\Delta},$$

[2]) D. Hilbert, loc. cit., S. 222.

so erhält man mit Hilfe der Multiplikation der Determinanten

$$D_1 = \begin{vmatrix} r^2 - r^{p-1} & , & r^4 - r^{p-1} & , & \ldots, & r^{p-3} - r^{p-1} \\ r^4 - r^{2(p-1)} & , & r^8 - r^{2(p-1)} & , & \ldots, & r^{2(p-3)} - r^{2(p-1)} \\ \ldots & & \ldots & & & \ldots \\ r^{2q} - r^{q(p-1)} & , & r^{4q} - r^{q(p-1)} & , & \ldots, & r^{q(p-3)} - r^{q(p-1)} \end{vmatrix}.$$

Diese Determinante läßt sich auf die folgende Form bringen:

$$D_1 = (-1)^q \begin{vmatrix} 1 & , & 1 & , & \ldots, & 1 \\ r^2 & , & r^4 & , & \ldots, & r^{p-1} \\ \ldots & & \ldots & & & \ldots \\ r^{2q} & , & r^{4q} & , & \ldots, & r^{q(p+1)} \end{vmatrix},$$

welche eine Vandermondesche Determinante ist, deren Wert also leicht ersichtlich nicht verschwindet. Demnach hat $D(\beta_1, \ldots, \beta_q)$ einen von Null verschiedenen Wert, und damit ist die Unabhängigkeit der Einheiten $\beta_1, \ldots, \beta_q$ bewiesen.

Wir wählen nun in (3) und (4) die primitive Wurzel r in solcher Weise, daß

$$r^{p-1} \equiv 1 \pmod{p^{\nu+1}} \tag{5}$$

gilt, was offenbar immer möglich ist. Wird e^v in die Form (3) der Kreiseinheiten ε_k anstatt ζ gesetzt, so erhalten wir mit Hilfe der bekannten Eulerschen Reihe

$$\log \frac{e^v - 1}{v} = \frac{v}{2} + \frac{B_1}{2.2!} v^2 - \frac{B_2}{4.4!} v^4 + \frac{B_3}{6.6!} v^6 - \ldots,$$

(wo $B_1, B_2, \ldots$ die Bernoullischen Zahlen bezeichnen), die folgende unendliche Reihe:

$$\log [\varepsilon_k(e^v)]^{p-1} = (p-1)\left\{\log r + (r^2-1)\frac{B_1}{2.2!} r^{2k} \cdot v^2 - \right.$$
$$\left. -(r^4-1)\frac{B_2}{4.4!} r^{4k} \cdot v^4 + (r^6-1)\frac{B_3}{6.6!} r^{6k} \cdot v^6 - \ldots \right\}.$$

Daraus ergibt sich für die Einheiten $\beta_1, \ldots, \beta_2$:

$$\log [\beta_j(e^v)]^{p-1} = (p-1)\left\{C + (r^2-1)\frac{B_1}{2.2!} v^2 \cdot \sum_{k=1}^{\frac{p-1}{2}} r^{2k(j+1)} - \right.$$
$$-(r^4-1)\frac{B_2}{4.4!} v^4 \sum_{k=1}^{\frac{p-1}{2}} r^{2k(j+2)} + (r^6-1)\frac{B_3}{6.6!} v^6 \sum_{k=1}^{\frac{p-1}{2}} r^{2k(j+3)} - \ldots \tag{6}$$
$$\left. (j = 1, 2, \ldots, q). \right.$$

wo C eine Konstante bedeutet. Schreibt man $i = \frac{p-1}{2} - j$, so gelten wegen (5)

$$\sum_{k=1}^{\frac{p-1}{2}} r^{2k(j+h)} \equiv 0 \pmod{p^{\nu+1}} \qquad \left(h = 1, 2, \ldots, p-2;\ h \neq i,\ i + \frac{p-1}{2}\right)$$

und

$$\sum_{k=1}^{\frac{p-1}{2}} r^{2k(j+i)} \equiv \frac{p-1}{2} \qquad (\mathrm{mod}\ p^{w+1}).$$

Wir bezeichnen kurz die x-te Ableitung der Funktion $\log \omega(e^v)$ an der Stelle $v=0$ durch $D_x \log \omega(e^v)$. Aus (6) erhalten wir die folgenden Kongruenzen

$$D_{hp^{u_i}} \log \beta_j^{p-1}(e^v) \equiv 0 \pmod{p^{u_i+1}} \quad (h = 1, 2, \ldots, 2i-1, 2i+1, \ldots, p-2),$$

und

$$D_{2ip^{u_i}} \log \beta_j^{p-1}(e^v) \equiv (-1)^{i+1} \cdot \frac{p-1}{2} \cdot (r^{2ip^{u_i}}-1) \cdot \frac{B_{ip^{u_i}}}{2ip^{u_i}} \pmod{p^{u_i+1}},$$

$$\left(i = 1, 2, \ldots, q;\ j = \frac{p-1}{2} - i\right),$$

da nach Definition $u_i \leqq w$ $(i = 1, \ldots, q)$ ist. Gemäß (1) ist $B_{ip^{u_i}}$ genau durch die $2u_i$-te Potenz von p teilbar.[3]) Es gilt also

(7a) $$D_{2ip^{u_i}} \log \beta_j^{p-1}(e^v) \not\equiv 0 \pmod{p^{u_i+1}} \quad (i = 1, \ldots, q),$$

jedoch

(7b) $$D_{tp^s} \log \beta_j^{p-1}(e^v) \equiv 0 \pmod{p^{s+1}},\ (s = 1, \ldots, u_i-1),\ (t = 1, \ldots, p-2).$$

Die Einheit β_j^{p-1} genügt auf Grund des Satzes 3 in[4]) der folgenden Kongruenz

(8) $$\beta_j^{p-1} \equiv a_0 + a_i \lambda^{u_i(p-1)+2i} \pmod{l^{u_i(p-1)+2i+1}}.$$

Den Wert von a_0 erhalten wir, wenn wir in die Grundform von β_j^{p-1} den Wert 1 anstatt ζ setzen. Diese Grundform ist aber nicht bekannt; setzt man 1 anstatt ζ in die Definitionsform von β_j^{p-1}, so erhält man die Zahl a_0',

---

[3]) Den Beweis verdanke ich einer freundlichen brieflichen Mitteilung von Herrn N. G. W. H. Beeger. Die bekannten Kummerschen Kongruenzen bezüglich der Bernoullischen Zahlen sind

$$k^a(1-k^b)^c \equiv 0 \qquad (\mathrm{mod}\ p^a,\ p^{ec}),$$

wo $p-1 \nmid a+1$, $b = b_1 p^{e-1}(p-1)$, $p \nmid b$, $(b_1, p-1) = 1$.

Das Symbol k^a bedeutet:

$$k^a = \frac{h^{a+1}}{a+1},$$

und $B_a = (-1)^{a-1} \cdot h^{2a}$. Setzt man hier $a = 2ip^j - 1$, $c = 1$, $m = \frac{p-1}{2}$ und $e = j+1$, so erhält man die Kongruenz

$$\frac{B_{ip^j}}{2ip^j} \equiv (-1)^{b_1 m} \frac{B_{(i+b_1 m)p^j}}{2(i+b_1 m)p^j} \qquad (\mathrm{mod}\ p^{j+1}),$$

also in unserem Falle, wenn $b_1 = 2i$, gemäß (1) auch

$$\frac{B_{ip^{u_i-1}}}{2ip^{u_i-1}} \equiv \frac{B_{ip^{u_i}}}{2ip^{u_i}} \equiv 0 \qquad (\mathrm{mod}\ p^{u_i}),$$

wodurch

$$B_{ip^{u_i}} \equiv 0 \qquad (\mathrm{mod}\ p^{2u_i})$$

bewiesen ist. Dagegen ist $B_{ip^{u_i}}$ laut Definition (16) durch p^{2u_i+1} nicht teilbar.

für welche gemäß dem Satz 4 in [4]) die Kongruenz

$$a_0' \equiv a_0 \pmod{p^{u_i+1}} \tag{9}$$

immer erfüllt wird, falls

$$D_{p^{u_i}(p-1)} \log \beta_j^{p-1}(e^z) \equiv 0 \pmod{p^{u_i}}$$

ist, d. h. in unserem Falle, falls

$$(r^{p^{u_i}(p-1)}-1) \cdot \sum_{k=1}^{\frac{p-1}{2}} r^{2k\left(j+\frac{p^{u_i}(p-1)}{2}\right)} \cdot \frac{B_{p^{u_i}(p-1)/2}}{p^{u_i}(p-1)} \equiv 0 \pmod{p^{u_i}}$$

gilt. Der Nenner der von

$$\frac{B_{p^{u_i}(p-1)/2}}{p^{u_i}(p-1)}$$

sei etwa durch p^h teilbar; die primitive Wurzel r können wir stets so wählen, daß

$$r^{p-1} \equiv 1 \pmod{p^{w+h}}$$

sei. Dann ist (9) erfüllt.

Den Wert von a_0' können wir folgenderweise ermitteln. Setzt man 1 anstatt ζ in (3), so gilt $\varepsilon_k(1) = r$, natürlich nur für die Form (3). Ferner ist

$$\beta_j^{p-1}(1) = a_0' = r^{(p-1)\sum_{k=1}^{\frac{p-1}{2}} r^{2kj}} \equiv 1 \pmod{p^{w+1}}.$$

Wegen (8) und (9) ist also

$$\beta_j^{p-1} \equiv 1 + a_i \lambda^{u_i(p-1)+2i} \pmod{\mathfrak{l}^{u_i(p-1)+2i+1}}. \tag{10}$$

Nach Satz 3 in [4]) ist

$$a_i \equiv (-1)^{i+1} \cdot \frac{p-1}{2} \frac{r^{2ip^{u_i}}-1}{2i \cdot (2i)!} \frac{B_{ip^{u_i}}}{p^{2u_i}} \pmod{p};$$

a_i ist also eine zu p prime Zahl und es gibt eine Zahl c_i, mit welcher $a_i \cdot c_i \equiv 1 \pmod{p}$ ist. Folglich ist

$$\eta_i = \beta_j^{(p-1)c_i} \qquad \left(j = \frac{p-1}{2} - i\right),$$

das i-te Glied in (2) und wenn i die Zahlen $1, 2, \ldots, q$ durchläuft, ergibt sich die Richtigkeit von (2).

Satz 2. *Ist p eine ungerade Primzahl vom Irregularitätsgrad w, und ε eine Einheit des zu p gehörigen Kreiskörpers $\Omega(\zeta)$, für welche die Kongruenzen*

$$D_{2ip^{u_i}} \log \varepsilon(e^z) \equiv 0 \pmod{p^{u_i+z}} \quad (i = 1, \ldots, q), \tag{11}$$

gelten (wo z eine natürliche Zahl ist und $u_1, \ldots, u_q$ das p-Charakter der Bernoullischen Zahlen bezeichnen), so ist ε die p^z-te Potenz einer Einheit in $\Omega(\zeta)$.

[4]) P. Dénes, Über die Kummerschen logarithmischen Hilfsfunktionen, *Acta Sci. Math. (Szeged)* **15** (1954), 115—125.

Beweis. Die Einheiten $\eta_{i_1}, \ldots, \eta_{i_q}$ aus (2) bilden eine unabhängige Einheitsschar aus $\frac{p-3}{2}$ Einheiten in $\Omega(\zeta)$, wonach die Einheit ε durch eine Gleichung

$$\varepsilon^d = \prod_{i=1}^{q} \eta_i^{d_i}$$

ausgedrückt werden kann, wo $d, d_1, \ldots, d_q$ ganze rationale Zahlen sind. Sind (11) erfüllt, so folgen wegen (7) — bei geeigneter Wahl der primitiven Wurzel r — die Kongruenzen

$$d_i \equiv 0 \pmod{p^z} \quad (i = 1, \ldots, q);$$

ε^d ist also eine volle p^z-te Potenz. Wäre nun d etwa durch p^m teilbar, und im allgemeinen $m > z$, so bildet man die Gleichung

$$\varepsilon^{dp^{-z}} = \prod_{i=1}^{q} \eta_i^{d_i p^{-z}}, \tag{12}$$

in welcher die Einheit $\varepsilon^{dp^{-z}}$ reell ist, da an der rechten Seite der Gleichung nur reelle Einheiten als Faktoren vorkommen. Hieraus folgt, daß in der Gleichung (12) durch die p^z-te Wurzelziehung keine primitive p-te Einheitswurzel auftritt. Die Wiederholung des obigen Verfahrens auf (12) zeigt, daß auch die Zahlen $d_i p^{-z}$ durch p^z teilbar sind. Die Fortsetzung der Methode ergibt also schließlich den vollständigen Beweis des Satzes, da man zu einer Gleichung

$$\varepsilon^{dp^{-m}} = \prod_{i=1}^{q} \eta_i^{d_i p^{-m}}$$

gelangt, in welcher die Exponenten $d_i p^{-m}$ sämtlich durch p^z teilbar sind.

Ähnlich zu Satz 2 erhalten wir leicht den folgenden Satz:

Satz 3. *Ist p eine ungerade Primzahl vom Irregularitätsgrad w und ε eine Einheit des zu p gehörigen Kreiskörpers $\Omega(\zeta)$, welche einer rationalen ganzen Zahl mod p^{w+z} kongruent ist, so ist ε die p^z-te Potenz einer Einheit in $\Omega(\zeta)$.*

Beweis. Aus der Kongruenz

$$\varepsilon \equiv c \pmod{p^{w+z}},$$

wo c eine ganze rationale Zahl ist, folgen nach dem Satz 2 in [4]) die folgenden Kongruenzen:

$$D_{jp^{w+z-1}} \log \varepsilon(e^v) \equiv 0 \pmod{p^{w+z}} \quad (j = 1, \ldots, p-2). \tag{13}$$

Die Kongruenzen (13) sind für ungerade Werte von j trivialerweise erfüllt, da ε eine reelle Einheit ist. Nun gilt nach [3])

$$\frac{B_{ip^{u_i+s}}}{2ip^{u_i+s}} \equiv \frac{B_{ip^{u_i+s+1}}}{2ip^{u_i+s+1}} \pmod{p^{u_i+1}}$$

für beliebige nicht negative ganze Zahlen s. Daraus folgt:

$$\frac{B_{ip^{u_i}}}{2ip^{u_i}} \equiv \frac{B_{ip^{w+z-1}}}{2ip^{w+z-1}} \pmod{p^{u_i+1}}.$$

Demnach erhalten wir

(14) $$D_{2ip^{w+z-1}} \log r_{i_i}(e^v) \equiv 0 \pmod{p^{u_i}},$$

jedoch

(15) $$D_{2ip^{w+z-1}} \log r_{i_i}(e^v) \not\equiv 0 \pmod{p^{u_i+1}}.$$

Auf Grund von (13), (14), (15) und $w \geqq u_i$ beendet man den Beweis ähnlich wie denjenigen des Satzes 2.

(Eingegangen am 25. November, 1952.)