ÜBER DIE CLASSENANZAHL

DER ZU EINER NEGATIVEN DETERMINANTE $D=-q$ GEHÖRIGEN EIGENTLICH PRIMITIVEN QUADRATISCHEN FORMEN WO q EINE PRIMZAHL VON DER FORM $4n+3$ IST

VON

JACOB HACKS
in MÜNCHEN.

Ist q eine Primzahl von der Form $4n+3$, so ist die Classenanzahl h der zu der Determinante $D=-q$ gehörigen eigentlich primitiven quadratischen Formen gleich dem Überschuss der Anzahl der zwischen o und $\frac{q}{2}$ liegenden quadratischen Reste von q über die Anzahl der zwischen o und $\frac{q}{2}$ liegenden quadratischen Nichtreste von q (Dirichlet, *Zahlentheorie*, 3. Auflage, p. 265), oder was dasselbe ist, gleich dem Überschuss der Anzahl der *unter* $\frac{q}{2}$ liegenden quadratischen Reste von q über die Anzahl der *über* $\frac{q}{2}$ liegenden quadratischen Reste von q. Bedeutet $[x]$ die grösste in einer Zahl x enthaltene ganze Zahl und setzt man

$$S=\sum_{s=1}^{s=\frac{q-1}{2}}\left[\frac{s^2}{q}\right],$$

$$S'=\sum_{s=1}^{s=\frac{q-1}{2}}\left[\frac{2s^2}{q}\right],$$

so ist die Anzahl ρ' der über $\frac{q}{2}$ liegenden quadratischen Reste von q gleich $S' - 2S$, wie sich leicht aus folgendem Satze ergibt: Liegt der kleinste positive Rest einer ganzen Zahl x nach dem Modul m unterhalb $\frac{m}{2}$, so ist $\left[\frac{2x}{m}\right] - 2\left[\frac{x}{m}\right] = 0$, ist derselbe $\geqq \frac{m}{2}$, so ist $\left[\frac{2x}{m}\right] - 2\left[\frac{x}{m}\right] = 1$ (Gauss' Werke, Band 2, p. 3). Die Anzahl ρ der *unter* $\frac{q}{2}$ liegenden quadratischen Reste von q ist demnach gleich $\frac{q-1}{2} - S' + 2S$. Hieraus ergibt sich für $h = \rho - \rho'$ der Ausdruck

$$h = \frac{q-1}{2} - 2S' + 4S. \tag{1}$$

Einen andern Ausdruck für h gewinnt man durch Anwendung eines in den Acta mathematica, Bd. 10, p. 18, begründeten Satzes, welcher lautet:

Eine Function $y = f(x)$ möge mit wachsendem x von $x = \mu$ bis $x = \mu'$ fortwährend zunehmen, wo μ und μ' ganze Zahlen bedeuten. Ferner sei $[f(\mu)] = \nu$, $[f(\mu')] = \nu'$ und $x = F(y)$ die aus $y = f(x)$ durch Umkehrung entstehende Function. Ist alsdann λ diejenige Zahl, welche angibt, wie viele unter den Functionswerten $f(\mu+1), f(\mu+2), \ldots, f(\mu')$ ganzzahlige Werte haben, so ist

$$\sum_{\mu+1}^{\mu'}[f(s)] + \sum_{\nu+1}^{\nu'}[F(s)] = -\mu\nu + \mu'\nu' + \lambda. \tag{2}$$

Wendet man diese Gleichung auf S an, so kommt

$$S + \sum_{1}^{\frac{q-3}{4}}[\sqrt{qs}] = \frac{(q-1)(q-3)}{8}. \tag{3}$$

Es geht dies daraus hervor, dass hier die in (2) mit λ bezeichnete Zahl verschwindet, und dass $\left[\frac{(q-1)^2}{4q}\right] = \frac{q-3}{4}$ ist. In ähnlicher Weise ergibt sich

$$S' + \sum_{1}^{\frac{q-3}{2}}\left[\sqrt{\frac{q}{2}s}\right] = \frac{q-1}{2}\,\frac{q-3}{2}. \tag{4}$$

Setzt man die aus (3) und (4) für S und S' sich ergebenden Werte in (1) ein, so wird

$$h = \frac{q-1}{2} + 2\sum_{1}^{\frac{q-3}{2}}\left[\sqrt{\frac{q}{2}s}\right] - 4\sum_{1}^{\frac{q-3}{4}}[\sqrt{qs}]. \tag{5}$$

Ohne Anwendung von Summenzeichen geschrieben lautet die Gleichung

$$\begin{aligned} h = \frac{q-1}{2} &+ 2\left(\left[\sqrt{\frac{q}{2}}\right] + \left[\sqrt{\frac{3q}{2}}\right] + \cdots + \left[\sqrt{\frac{q-5}{2}\frac{q}{2}}\right]\right) \\ &+ 2\left([\sqrt{q}] + [\sqrt{2q}] \qquad + \cdots + \left[\sqrt{\frac{q-3}{4}q}\right]\right) \\ &- 4\left([\sqrt{q}] + [\sqrt{2q}] \qquad + \cdots + \left[\sqrt{\frac{q-3}{4}q}\right]\right) \end{aligned}$$

oder

$$\begin{aligned} h = \frac{q-1}{2} &+ 2\left(\left[\sqrt{\frac{q}{2}}\right] - [\sqrt{q}] + \left[\sqrt{\frac{3q}{2}}\right] - [\sqrt{2q}] + \cdots \right. \\ &\left. + \left[\sqrt{\frac{q-5}{2}\frac{q}{2}}\right] - \left[\sqrt{\frac{q-3}{4}q}\right]\right),\text{[1]} \end{aligned} \tag{6}$$

$$h = \frac{q-1}{2} - 2\sum_{1}^{\frac{q-3}{2}}(-1)^s\left[\sqrt{\frac{q}{2}s}\right]. \tag{7}$$

Da h als Classenanzahl stets positiv ist, so folgt aus (6) die Ungleichheit

$$\begin{aligned} &[\sqrt{q}] - \left[\sqrt{\frac{q}{2}}\right] + [\sqrt{2q}] - \left[\frac{3q}{2}\right] + \cdots \\ &+ \left[\sqrt{\frac{q-3}{4}q}\right] - \left[\sqrt{\frac{q-5}{2}\frac{q}{2}}\right] \leqq \frac{q-3}{4}. \end{aligned} \tag{8}$$

Wir stellen jetzt für Primzahlen von der Form $4n+1$ eine ähnliche Betrachtung an. Auch für Primzahlen p von der Form $4n+1$ hat der

[1] Herr Geh. Regierungs-Rat LIPSCHITZ hat mich vor längerer Zeit auf diese Umformung aufmerksam gemacht.

Überschuss $\rho - \rho'$ der Anzahl der *unter* $\frac{p}{2}$ liegenden quadratischen Reste über die Anzahl der *über* $\frac{p}{2}$ liegenden quadratischen Reste den Ausdruck

$$\rho - \rho' = \frac{p-1}{2} - 2S' + 4S,$$

wo in S und S' statt q überall p zu setzen ist. Es gelten jetzt die Gleichungen

$$S + \sum_{1}^{\frac{p-1}{4}} [\sqrt{sp}] = \frac{(p-1)^2}{8},$$

$$S' + \sum_{1}^{\frac{p-1}{2}} \left[\sqrt{s\frac{p}{2}}\right] = \frac{(p-1)^2}{4}.$$

Da für Primzahlen von der Form $4n+1$ die Differenz $\rho - \rho'$ verschwindet, so ergibt sich

$$\frac{p-1}{2} + 2\sum_{1}^{\frac{p-1}{2}} \left[\sqrt{s\frac{p}{2}}\right] - 4\sum_{1}^{\frac{p-1}{4}} [\sqrt{sp}] = 0,$$

und hieraus

$$(9) \qquad [\sqrt{p}] - \left[\sqrt{\frac{p}{2}}\right] + [\sqrt{2p}] - \left[\sqrt{3\frac{p}{2}}\right] + \cdots$$
$$+ \left[\sqrt{\frac{p-1}{4}p}\right] - \left[\sqrt{\frac{p-3}{2}\frac{p}{2}}\right] = \frac{p-1}{4}.$$

Diese Gleichung hat mit der Ungleichheit (8) eine grosse Ähnlichkeit. Fasst man auf der linken Seite immer je zwei aufeinanderfolgende Glieder in einen Term zusammen, so hat in (8) jeder Term durchschnittlich einen Wert, welcher $\leqq 1$ ist, während in (9) jeder Term durchschnittlich den Wert 1 hat.

Die Gleichung (9) behält ihre Gültigkeit auch für solche Zahlen m, welche aus lauter verschiedenen Primzahlen von der Form $4n+1$ zusammengesetzt sind. Der Beweis ist leicht zu führen.

Der Ausdruck (7) für die Classenanzahl h kann weiter umgeformt werden mit Hülfe der im 10. Bande der Acta mathematica p. 19 aufgestellten Transformationsgleichung (3), welche unter Beibehaltung der in der obigen Gleichung (2) angewandten Notation folgende Gestalt hat:

$$\sum_{\mu+1}^{\mu'}[f(s)]\varphi(s)+\sum_{\nu+1}^{\nu'}\Psi[F(s)]=-\nu\Psi(\mu)+\nu'\Psi(\mu')$$
$$+\varphi(s_1)+\varphi(s_2)+\ldots+\varphi(s_\lambda).$$

Hier bezeichnet $\varphi(s)$ eine beliebige Function, ferner sind $s_1, s_2, \ldots, s_\lambda$ diejenigen ganzzahligen zwischen $\mu+1$ und μ' mit Einschluss beider Grenzen liegenden Argumente, für welche die Function $y=f(x)$ einen ganzzahligen Wert erhält, und es ist $\Psi(s)=\sum\limits_1^s\varphi(s)$.

Setzt man in dieser Transformationsgleichung

$$\varphi(s)[f(s)]=(-1)^s\left[\sqrt{\frac{q}{2}s}\right]$$

und bedenkt, dass die Zahl λ verschwindet, so ergibt sich leicht

$$\sum_1^{\frac{q-3}{2}}(-1)^s\left[\sqrt{\frac{q}{2}s}\right]+\sum_1^{\frac{q-3}{2}}\sum_1^{\left[\frac{2s^2}{q}\right]}(-1)^s=\frac{q-3}{2}\sum_1^{\frac{q-3}{2}}(-1)^s.$$

Da $\frac{q-3}{2}=2n$ eine gerade Zahl ist, so ist

$$\sum_1^{\frac{q-3}{2}}(-1)^s=0,$$

also

$$\sum_1^{\frac{q-3}{2}}(-1)^s\left[\sqrt{\frac{q}{2}s}\right]+\sum_1^{\frac{q-3}{2}}\sum_1^{\left[\frac{2s^2}{q}\right]}(-1)^s=0.$$

Demnach erhält die Classenanzahl h den Ausdruck

$$h=\frac{q-1}{2}+2\sum_1^{\frac{q-3}{2}}\sum_1^{\left[\frac{2s^2}{q}\right]}(-1)^s.$$

Um für S' einen andern Ausdruck zu gewinnen, stellen wir folgende Reihen von Gleichungen auf:

$$2\,.\,1^2 = \left[\frac{2\,.\,1^2}{q}\right]q + r_1,$$

$$2\,.\,2^2 = \left[\frac{2\,.\,2^2}{q}\right]q + r_2,$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$2\,.\left(\frac{q-1}{2}\right)^2 = \left[\frac{2\,.\left(\frac{q-1}{2}\right)^2}{q}\right]q + r_{\frac{q-1}{2}}.$$

Durch Addition dieser Gleichungen erhält man

$$2\sum_1^{\frac{q-1}{2}} s^2 = S'q + \sum_1^{\frac{q-1}{2}} r_s.$$

Nach einer bekannten Formel ist

$$\sum_1^{\frac{q-1}{2}} s^2 = \frac{q(q^2-1)}{24}.$$

Bezeichnet man die Summe der Reste $(\operatorname{mod} q)$ mit R, die Summe der Nichtreste mit R', so ist $\sum r_s = R$ oder $= R'$, je nachdem q von der Form $8n + 7$ oder von der Form $8n + 3$ ist. Es folgt dies aus dem Umstande, dass die Zahl 2 quadratischer Rest ist von den Primzahlen $q = 8n + 7$, quadratischer Nichtrest von den Primzahlen $q = 8n + 3$. Es sei nun zunächst die Primzahl q von der Form $8n + 7$, so ergibt sich

$$S' = \frac{q^2-1}{12} - \frac{R}{q}.$$

In ganz derselben Weise findet man (s. Acta mathematica, Bd. 10, p. 45)

$$S = \frac{q^2-1}{24} - \frac{R}{q}.$$

Setzt man diese Werte in die Gleichung (1) ein, so kommt

$$h = \frac{q-1}{2} - \frac{2R}{q},$$

oder mit Berücksichtigung der Relation

$$R + R' = \frac{q(q-1)}{2},$$

(10)
$$h = \frac{R' - R}{q}.$$

Ist q eine Primzahl von der Form $8n + 3$, so findet man

$$S' = \frac{q^2 - 1}{12} - \frac{R'}{q},$$

$$S = \frac{q^2 - 1}{24} - \frac{R}{q},$$

$$h = \frac{q-1}{2} - \frac{4R}{q} + \frac{2R'}{q}$$

$$= 3\left(\frac{q-1}{2} - \frac{2R}{q}\right)$$

oder

(11)
$$h = 3\,\frac{R' - R}{q}.$$

Die Gleichungen (10) und (11) lassen sich vereinigen in die Formel

(12)
$$h = \left[2 - \left(\frac{2}{q}\right)\right]\frac{R' - R}{q},$$

wo $\left(\frac{2}{q}\right)$ das Legendre'sche Zeichen ist, (DIRICHLET, *Zahlentheorie,* p. 263). Aus (12) geht hervor, dass die Summe der Nichtreste grösser ist, als die Summe der Reste (cf. BOUNIAKOWSKY, *Démonstration de quelques propositions relatives à la fonction numérique* $E(x)$, Bulletin de l'Académie de St. Pétersbourg, tome 28, p. 425).

Zwischen den Zahlen ρ und ρ' einerseits und den Summen R und

R' andererseits finden sehr einfache Beziehungen statt. Ist nämlich q eine Primzahl von der Form $8n + 7$, so ist

$$S' - 2S = \frac{R}{q},$$

und da auch

$$S' - 2S = \rho'$$

ist, so findet man

$$R = q\rho'$$

und vermöge der Relation

$$R + R' = \frac{q(q-1)}{2} = q(\rho + \rho'),$$

$$R' = q\rho.$$

Ist q von der Form $8n + 3$, so findet man auf die nämliche Weise

$$2R' - R = q\rho,$$

$$2R - R' = q\rho'.$$