Über die Wertverteilung des Jacobischen Symbols.

Von L. RÉDEI in Szeged.

Bezeichne $m(>1)$ eine ungerade quadratfreie natürliche Zahl und $\left(\frac{a}{m}\right)$ das Symbol von JACOBI. Wir nennen die Summe

$$(1) \qquad (\alpha, \beta)_m = \sum_{\alpha \leqq x \leqq \beta} \left(\frac{x}{m}\right)$$

den (quadratischen) Exzeß des Intervalls (α, β).

Man teile das Intervall $(0, m)$ in 8, 10 bzw. 12 gleiche Intervalle ein und bezeichne den Exzeß der Reihe nach bzw. mit

$$(2) \qquad A_1, \ldots, A_8;\; B_1, \ldots, B_{10};\; C_1, \ldots, C_{12}.$$

Die Klassenzahl des quadratischen Zahlkörpers von $\sqrt{-km}$ bezeichnen wir mit h_k, dabei wollen wir für k nur solche natürlichen Zahlen zulassen, für die auch km quadratfrei ist. (In der Wirklichkeit werden bei uns nur h_1, h_2, h_3, h_5 vorkommen.)

Bekanntlich lauten die Klassenzahlformeln von DIRICHLET so:

$$(3) \qquad h_1 = \begin{cases} 2(A_1+A_2), \\ A_1+\ldots+A_4, \end{cases} \quad h_2 = \begin{cases} 2(A_1-A_4) & (m\equiv 1 \pmod 4)), \\ 2(A_2+A_3) & (m \equiv 3 \pmod 4)). \end{cases}$$

Dies hat auch die berühmte, arithmetisch noch nicht bewiesene Folgerung, daß die Linearkombinationen der A_i auf den rechten Seiten in (3) positiv sind.

Auf Grund von (3) lassen sich umgekehrt die A_i durch h_1, h_2 leicht ausdrücken, wie das schon GAUSS bemerkt hat. Außerdem fand er, daß sich die C_i im Falle $3 \nmid m$ durch h_1, h_3 berechnen lassen, den Beweis hat man von DIRICHLET.[1]) Wir werden die B_i im Falle $5 \nmid m$, $m \equiv 3 \pmod 4$ durch h_1, h_5 bestimmen (für $m \equiv 1 \pmod 4$ ist das uns nicht gelungen). Wir halten diesen kleinen Fortschritt schon aus dem Grunde der Veröffentlichung wert, da 10-Teilung im allgemeinen nicht so leicht ist wie 8-Teilung oder 12-Teilung. Auch lassen sich aus allen diesen Resultaten einige theoretisch und praktisch interessante Folgerungen ziehen, wie wir das später unten bemerken werden.

---

[1]) S. hierüber die Bemerkungen von DEDEKIND in GAUSS's *Werke* II (1876), S. 301–303.

Wir stellen alle die genannten Formeln, die alten und die neuen zusammen:

$$\left.\begin{aligned}
A_1 = A_8 &= \frac{1}{4}\left(\frac{2}{m}\right) h_1 + \frac{1}{4} h_2 \\
A_2 = A_7 &= \frac{1}{4}\left(2 - \left(\frac{2}{m}\right)\right) h_1 - \frac{1}{4} h_2 \\
A_3 = A_6 &= -\frac{1}{4}\left(2 + \left(\frac{2}{m}\right)\right) h_1 + \frac{1}{4} h_2 \\
A_4 = A_5 &= \frac{1}{4}\left(\frac{2}{m}\right) h_1 - \frac{1}{4} h_2
\end{aligned}\right\}\quad (m \equiv 1 \pmod 4),$$

$$\left.\begin{aligned}
A_1 = -A_8 &= \frac{1}{4}\left(3 + \left(\frac{2}{m}\right)\right) h_1 - \frac{1}{4} h_2 \\
A_2 = -A_7 &= -\frac{1}{4}\left(1 - \left(\frac{2}{m}\right)\right) h_1 + \frac{1}{4} h_2 \\
A_3 = -A_6 &= \frac{1}{4}\left(1 - \left(\frac{2}{m}\right)\right) h_1 + \frac{1}{4} h_2 \\
A_4 = -A_5 &= \frac{1}{4}\left(1 - \left(\frac{2}{m}\right)\right) h_1 - \frac{1}{4} h_2
\end{aligned}\right\}\quad (m \equiv 3 \pmod 4),$$

$$\left.\begin{aligned}
B_1 = -B_{10} &= \frac{1}{12}\left(7 + 5\left(\frac{2}{m}\right) + \left(\frac{5}{m}\right) - \left(\frac{10}{m}\right)\right) h_1 - \frac{1}{12}\left(1 + \left(\frac{2}{m}\right)\right) h_5 \\
B_2 = -B_9 &= \frac{1}{4}\left(1 - \left(\frac{5}{m}\right)\right) h_1 - \frac{1}{12}\left(1 - 2\left(\frac{2}{m}\right)\right) h_5 \\
B_3 = -B_8 &= -\frac{1}{4}\left(1 - \left(\frac{5}{m}\right)\right) h_1 + \frac{1}{4} h_5 \\
B_4 = -B_7 &= \frac{1}{4}\left(1 - \left(\frac{5}{m}\right)\right) h_1 + \frac{1}{12}\left(1 - 2\left(\frac{2}{m}\right)\right) h_5 \\
B_5 = -B_6 &= \frac{1}{12}\left(2 - 5\left(\frac{2}{m}\right) + 2\left(\frac{5}{m}\right) + \left(\frac{10}{m}\right)\right) h_1 - \frac{1}{12}\left(2 - \left(\frac{2}{m}\right)\right) h_5
\end{aligned}\right\}\quad (5 \nmid m;\ m \equiv 3 \pmod 4),$$

$$\left.\begin{aligned}
C_1 = C_{12} &= \frac{1}{4}\left(1 + \left(\frac{3}{m}\right)\right) h_1 + \frac{1}{12}\left(1 + \left(\frac{2}{m}\right)\right) h_3 \\
C_2 = C_{11} &= -\frac{1}{4}\left(1 + \left(\frac{3}{m}\right)\right) h_1 + \frac{1}{12}\left(1 + \left(\frac{2}{m}\right)\right) h_3 \\
C_3 = C_{10} &= \frac{1}{2} h_1 - \frac{1}{6}\left(1 + \left(\frac{2}{m}\right)\right) h_3 \\
C_4 = C_9 &= -\frac{1}{2} h_1 + \frac{1}{6}\left(2 - \left(\frac{2}{m}\right)\right) h_3 \\
C_5 = C_8 &= \frac{1}{4}\left(1 + \left(\frac{3}{m}\right)\right) h_1 - \frac{1}{12}\left(5 - \left(\frac{2}{m}\right)\right) h_3 \\
C_6 = C_7 &= -\frac{1}{4}\left(1 + \left(\frac{3}{m}\right)\right) h_1 + \frac{1}{12}\left(1 + \left(\frac{2}{m}\right)\right) h_3
\end{aligned}\right\}\quad (3 \nmid m;\ m \equiv 1 \pmod 4).$$

$$\left.\begin{aligned}
C_1 = -C_{12} &= \frac{1}{12}\left(9+3\left(\frac{2}{m}\right)-\left(\frac{3}{m}\right)+\left(\frac{6}{m}\right)\right)h_1-\frac{1}{4}h_3\\
C_2 = -C_{11} &= -\frac{1}{4}\left(1-\left(\frac{2}{m}\right)-\left(\frac{3}{m}\right)+\left(\frac{6}{m}\right)\right)h_1+\frac{1}{4}h_3\\
C_3 = -C_{10} &= \frac{1}{6}\left(-\left(\frac{3}{m}\right)+\left(\frac{6}{m}\right)\right)h_1\\
C_4 = -C_9 &= \frac{1}{6}\left(3-2\left(\frac{3}{m}\right)-\left(\frac{6}{m}\right)\right)h_1\\
C_5 = -C_8 &= -\frac{1}{4}\left(1+\left(\frac{2}{m}\right)-\left(\frac{3}{m}\right)-\left(\frac{6}{m}\right)\right)h_1+\frac{1}{4}h_3\\
C_6 = -C_7 &= \frac{1}{12}\left(3-3\left(\frac{2}{m}\right)+\left(\frac{3}{m}\right)-\left(\frac{6}{m}\right)\right)h_1-\frac{1}{4}h_3
\end{aligned}\right\}\quad (3\nmid m;\ m\equiv 3 \pmod 4)).$$

Unser Beweis beruht auf folgendem einfachen Prinzip: Bezeichne k jetzt eine zu m prime natürliche Zahl. Man teile die ganzen Zahlen des Intervalls (α, β) in k Klassen ein, so daß die Zahlen der i-ten Klasse $\equiv -im \pmod k$ sind $(i=0, \ldots, k-1)$. Addiert man im zu den Zahlen der i-ten Klasse, so erhält man die durch k teilbaren ganzen Zahlen des Intervalls $(im+\alpha, im+\beta)$, d. h. die k-fachen der ganzen Zahlen des Intervalls $\left(\frac{im+\alpha}{k}, \frac{im+\beta}{k}\right)$.

Einerseits folgt hieraus sofort

$$(4)\qquad (\alpha, \beta)_m = \left(\frac{k}{m}\right)\sum_{i=0}^{k-1}\left(\frac{im+\alpha}{k}, \frac{im+\beta}{k}\right)_m \qquad ((k, m)=1).$$

Andererseits wenn km sogar ungerade und quadratfrei ist, so folgt aus obigem ebenso leicht

$$(\alpha, \beta)_{km} = \left(\frac{k}{m}\right)\sum_{i=0}^{k-1}\left(\frac{-im}{k}\right)\left(\frac{im+\alpha}{k}, \frac{im+\beta}{k}\right)_m.$$

Der Summand verschwindet für $i=0$. Wird auch

$$\left(\frac{k}{m}\right)\left(\frac{m}{k}\right) = \left(\frac{-1}{k}\right)^{\frac{m-1}{2}}$$

berücksichtigt, so folgt

$$(5)\qquad (\alpha, \beta)_{km} = \left(\frac{-1}{k}\right)^{\frac{m+1}{2}}\sum_{i=1}^{k-1}\left(\frac{i}{k}\right)\left(\frac{im+\alpha}{k}, \frac{im+\beta}{k}\right)_m.$$
$$(km \text{ quadratfrei},\ 2\nmid km).$$

Aus diesen Gleichungen (4), (5) und aus den trivialen Beziehungen

$$(6)\qquad (\alpha, \beta)_m = \left(\frac{-1}{m}\right)(-\beta, -\alpha),$$

$$(7)\qquad (\alpha, \beta)_m = (\alpha', \beta')_m \qquad (\alpha\equiv\alpha';\ \beta\equiv\beta' \pmod m))$$

ließen sich alle obigen Formeln beweisen, wir führen aber den Beweis nur für B_i aus, da die übrigen Formeln bekannt sind.

Vor allem sind unsere Behauptungen $B_i = -B_j$ $(i+j=11)$ wegen (6) richtig. Deshalb brauchen wir nur die $B_1, \ldots, B_5$ zu berechnen.

Zunächst gilt nach (3)

$$B_1+B_2+B_3+B_4+B_5=h_1. \tag{8}$$

Wir wenden (4) dreimal an (der Reihe nach mit $k=2,2,5$):

$$\left(0, \frac{m}{5}\right)_m = \left(\frac{2}{m}\right) \sum_{i=0}^{1} \left(\frac{im}{2}, \frac{im}{2}+\frac{m}{10}\right)_m = \left(\frac{2}{m}\right) \sum_{i=0}^{1} \left(\frac{5i}{10}m, \frac{5i+1}{10}m\right)_m,$$

$$\left(\frac{m}{5}, \frac{2m}{5}\right)_m = \left(\frac{2}{m}\right) \sum_{i=0}^{1} \left(\frac{im}{2}+\frac{m}{10}, \frac{im}{2}+\frac{2m}{10}\right)_m = \left(\frac{2}{m}\right) \sum_{i=0}^{1} \left(\frac{5i+1}{10}m, \frac{5i+2}{10}m\right)_m,$$

$$\left(0, \frac{m}{2}\right)_m = \left(\frac{5}{m}\right) \sum_{i=0}^{4} \left(\frac{im}{5}, \frac{im}{5}+\frac{m}{10}\right)_m = \left(\frac{5}{m}\right) \sum_{i=0}^{4} \left(\frac{2i}{10}m, \frac{2i+1}{10}m\right)_m.$$

Durch die B_i ausgedrückt:

$$B_1+B_2=\left(\frac{2}{m}\right)(B_1+B_6)=\left(\frac{2}{m}\right)(B_1-B_5),$$

$$B_3+B_4=\left(\frac{2}{m}\right)(B_2+B_7)=\left(\frac{2}{m}\right)(B_2-B_4),$$

$$h_1=\left(\frac{5}{m}\right)(B_1+B_3+B_5+B_7+B_9)=\left(\frac{5}{m}\right)(B_1-B_2+B_3-B_4+B_5).$$

Also gelten

$$\left(1-\left(\frac{2}{m}\right)\right)B_1+B_2+\left(\frac{2}{m}\right)B_5=0, \tag{9}$$

$$B_2-\left(\frac{2}{m}\right)B_3-\left(1+\left(\frac{2}{m}\right)\right)B_4=0, \tag{10}$$

$$B_1-B_2+B_3-B_4+B_5=\left(\frac{5}{m}\right)h_1. \tag{11}$$

Endlich wenden wir (5) mit $k=5$ an:

$$\left(0, \frac{5m}{2}\right)_{5m} = \sum_{i=1}^{4} \left(\frac{i}{5}\right) \left(\frac{im}{5}, \frac{im}{5}+\frac{5m}{10}\right)_m.$$

Die linke Seite ist nach (3) gleich h_5, und so folgt

$$h_5=(B_3+B_4+B_5+B_6+B_7)-(B_5+B_6+B_7+B_8+B_9)-$$
$$-(B_7+B_8+B_9+B_{10}+B_1)+(B_9+B_{10}+B_1+B_2+B_3).$$

Nach leichten Vereinfachungen:

$$h_5=B_3-(-B_4-B_3-B_2)-(-B_4-B_3-B_2)+B_3.$$

Folglich haben wir

$$B_2+2B_3+B_4=\frac{1}{2}h_5. \tag{12}$$

Aus (8)–(12) folgen die behaupteten Formeln für die B_i, womit unser Beweis beendet ist.

B e m e r k u n g e n. Wir betrachten den Fall $\left(\frac{-1}{m}\right)=-1$, $3\nmid m$, $5\nmid m$ (z. B. kann m eine Primzahl $\equiv 3 \pmod 4$ und größer als 3 sein). Alle Endpunkte der obengenannten 8-, 10-, 12-Teilungen des Intervalls $(0, m)$ zerlegen dieses Intervall in 24 Teilintervalle, die wir in natürlicher Reihenfolge mit $I_1, \ldots, I_{24}$ bezeichnen, entsprechend soll der Exzeß mit $E_1, \ldots, E_{24}$ bezeichnet werden. Es genügt nur die $I_1, \ldots, I_{12}$ und $E_1, \ldots, E_{12}$ zu betrachten. Jedem dieser Intervalle $I_1, \ldots, I_{12}$ schreiben wir die Länge darunter:

I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9	I_{10}	I_{11}	I_{12}
$\frac{m}{12}$	$\frac{m}{60}$	$\frac{m}{40}$	$\frac{m}{24}$	$\frac{m}{30}$	$\frac{m}{20}$	$\frac{m}{20}$	$\frac{m}{30}$	$\frac{m}{24}$	$\frac{m}{40}$	$\frac{m}{60}$	$\frac{m}{12}$.

Aus obigem folgt, daß sich alle Exzesse E_i in der Form

$$\nu h_1 + \varrho h_2 + \sigma h_3 + \tau h_5$$

ausdrücken lassen. Wegen $h_k > 0$ läßt sich auf diesem Wege unter Umständen auf das Vorzeichen von E_i schließen. (Auch führt dieser Weg zu einer leichteren Berechnung der Klassenzahlen h_k.) So gewinnen wir z. B. folgende Aussagen:

Für $m \equiv 19, 91 \pmod{120}$ ist $E_2 = \frac{1}{4} h_3 > 0$. (Wegen $h_3 = 4E_2$ genügt es jetzt zur Bestimmung von h_3 den Exzeß E_2 des Intervalls $I_2 = \left(\frac{m}{12}, \frac{m}{10}\right)$ von der Länge $\frac{m}{60}$ zu berechnen.)

Es gilt für den Exzeß des Intervalls $I_7 = \left(\frac{m}{4}, \frac{3m}{10}\right)$ von der Länge $\frac{m}{20}$:

$$E_7 = \frac{1}{12}\left(1-\left(\frac{2}{m}\right)\right)\left(1+\left(\frac{5}{m}\right)\right) h_1 + \frac{1}{12}\left(1+\left(\frac{2}{m}\right)\right) h_5 \geqq 0$$
$$(m \equiv 3 \pmod 4;\ 5 \nmid m).$$

(Hier ist auch $3|m$ zugelassen.)

Für $m \equiv 31, 79 \pmod{120}$ ist das Vorzeichen von $E_4, E_5, E_6, E_7, E_8, E_9$ der Reihe nach $+ - + + - +$ (vier Vorzeichenwechsel!). Selbst diese Exzesse sind nämlich gleich:

$$\frac{1}{4} h_1,\ -\frac{1}{12} h_5,\ \frac{1}{12} h_5,\ \frac{1}{6} h_5,\ -\frac{1}{6} h_5,\ \frac{1}{4} h_1.$$

(Eingegangen am 22. Oktober 1950.)