Über den quadratischen Restcharakter

von

Leopold Gegenbauer,

c. M. k. Akad.

Ich habe vor Kurzem¹ die Relationen

$$\left(\frac{m_1}{m_0}\right) = (-1)^{\sum_{x=1}^{x=m_1-1} \left[\frac{x m_0}{2 m_1} + \frac{1}{2}\right]} \quad 1)$$

$$\left(\frac{m_1}{m_0}\right) = (-1)^{\sum_{x=1}^{x=\frac{m_1-1}{2}} \left[\frac{(2x-1)m_0}{2 m_1} + \frac{1}{2}\right]} \quad 2)$$

bewiesen, von denen die erste, wie meine Ableitung zeigt, auch für gerade m_1 gilt. In dieser Mittheilung sollen nun aus diesen Gleichungen einige bemerkenswerthe Folgerungen gezogen werden. Die zweite von ihnen lässt sich übrigens, wie ich hier zeigen will, unter Benützung des quadratischen Reciprocitätsgesetzes unmittelbar aus der bekannten Gleichung

$$(m_0, m_1) = \sum_{x=1}^{x=\frac{m_1-1}{2}} \left[\frac{x m_0}{m_1}\right]$$

ableiten. Setzt man in derselben nämlich

$$x = \frac{m_1 + 1}{2} - x_1,$$

¹ „Note über das Legendre-Jacobi'sche Symbol.“ Diese Sitzungsber. Bd. 100, Abth. II. a., S. 855—864.

so erhält man

$$(m_0, m_1) = \frac{(m_0-1)(m_1-1)}{4} + \sum_{x=1}^{x=\frac{m_1-1}{2}} \left[\frac{1}{2} - \frac{(2x-1)m_0}{2m_1} \right]$$

oder, da für jedes nicht ganzzahlige α

$$[-\alpha] = -1 - [\alpha]$$

ist,

$$(m_0, m_1) + \sum_{x=1}^{x=\frac{m_1-1}{2}} \left[\frac{(2x-1)m_0}{2m_1} + \frac{1}{2} \right] = \frac{(m_0-1)(m_1-1)}{4},$$

durch welche Gleichung die eben gemachte Behauptung erhärtet wird.

Der einfachste Fall der Gleichung 1), welcher besagt, dass die durch das Kronecker-Schering'sche Lemma definierte charakterische Zahl $(2, m_0)$ von 2 in Bezug auf eine ungerade Zahl m_0 gleich der an $\frac{m_0}{4}$ zunächst liegenden ganzen Zahl ist, ist längst bekannt. Zu dieser höchst interessanten Bestimmung eines quadratischen Restcharakters mit Hilfe einer einzigen nächsten ganzen Zahl wurden später von Herrn V. Buniakowsky¹ und mir² noch die weiteren derselben Kategorie angehörigen Relationen

$$\left(\frac{3}{m_0}\right) = (-1)^{\left[\frac{m_0}{6} + \frac{1}{2}\right]}$$

$$\left(\frac{6}{m_0}\right) = (-1)^{\left[\frac{m_0}{12} + \frac{1}{2}\right]}$$

$$\left(\frac{5}{m_0}\right) = (-1)^{\left[\frac{m_0}{5} + \frac{1}{2}\right]}$$

¹ „Sur les congruences binômes exponentielles à base 3 et sur plusieurs nouveaux théorèmes relatifs aux résidus et aux racines primitives.“ Bulletin de l'académie impériale des sciences de St. Pétersburg. T. XIV, p. 356–381.

² „Über das Legendre-Jacobi'sche Symbol.“ Diese Sitzungsber., Bd. 91, Abth. II, S. 11–33.

hinzugefügt, deren erste den speciellsten Fall der Gleichung 2) repräsentirt. Noch weitere ebenso einfache Ausdrücke bei beliebigem ungeraden m_0 vermochte ich bisher nur für einige wenige mit den eben angeführten im engsten Zusammenhange stehende Legendre-Jacobi'sche Symbole, wie beispielsweise $\left(\frac{m_0}{2rm_0 \pm 3}\right)$, $\left(\frac{m_0}{2rm_0 \pm 5}\right)$ zu ermitteln. Aus den Gleichungen 1) und 2) kann man nun für eine Reihe von quadratischen Restcharakteren Darstellungen mit Hilfe von zwei nächsten ganzen Zahlen erschliessen, von denen ich am zuletzt angeführten Orte schon die durch die Relation

$$\left(\frac{7}{m_0}\right) = (-1)^{\left[\frac{m_0}{14} + \frac{1}{2}\right] + \left[\frac{m_0}{7} + \frac{1}{2}\right]}$$

gegebene ohne Beweis mitgetheilt habe, zu welcher in den folgenden Zeilen noch einige andere hinzugefügt werden sollen.

Berücksichtigt man übrigens, dass $\left[\frac{m_0}{7} + \frac{1}{2}\right]$ für alle zu 7 theilerfremden ungeraden Zahlen m_0 , welche nicht die Form $14t \pm 5$ besitzen, gerade für diese aber ungerade ist, so sieht man, dass für alle ungeraden Zahlen m_0 von einer der vier Formen $14t \pm 1$, $14t \pm 3$ die den vorangeführten Gleichungen vollkommen entsprechende Relation

$$\left(\frac{7}{m_0}\right) = (-1)^{\left[\frac{m_0}{14} + \frac{1}{2}\right]}$$

besteht, während für die Zahlen m_0 von einer der beiden Formen $14t \pm 5$

$$\left(\frac{7}{m_0}\right) = -(-1)^{\left[\frac{m_0}{14} + \frac{1}{2}\right]}$$

ist. Ähnliche einfache Resultate erlangt man auch in anderen Fällen, wenn man entweder m_1 nicht allgemein, sondern von geeigneter Form annimmt, oder m_0 passend wählt, wie an einigen Beispielen gezeigt werden wird.

Die im Anfange erwähnten Gleichungen 1) und 2) nebst der Formel

$$\left(\frac{m_1}{m_0}\right) = (-1)^{\sum_{x=1}^{x=m_1-1} \left[\frac{xm_0}{2m_1}\right]} \quad (2a)$$

unterscheiden sich von den übrigen bisher gebrauchten Darstellungen des quadratischen Restcharakters mit Hilfe von grössten ganzen Zahlen dadurch, dass bei ihnen der Nenner des Legendre-Jacobi'schen Symbols in den Zählern der auftretenden Ausdrücke vorkommt, wesshalb sich aus ihnen mit Leichtigkeit einfache Algorithmen zur Bestimmung dieses Zeichens ableiten lassen, von denen einer hier angegebenen werden mag.

Die ungerade Zahl m_0 , welche zu m_1 theilerfremd ist, kann stets auf die Form

$$m_0 = 2m_1 t_1 \pm m_2 \quad (3)$$

gebracht werden, wo m_2 positiv, ungerade, kleiner als m_1 und zu dieser Zahl relativ prim ist. Führt man diesen Werth von m_0 in die Gleichungen 1) und 2) ein, so verwandeln sich dieselben in

$$\left(\frac{m_1}{m_0}\right) = (-1)^{\left[\frac{m_1}{2}\right] t_1 + \sum_{x=1}^{x=m_1-1} \left[\frac{1}{2} + \frac{xm_2}{2m_1}\right]} \quad (4)$$

$$\left(\frac{m_1}{m_0}\right) = (-1)^{\left[\frac{m_1}{2}\right] t_1 + \sum_{x=1}^{x=\frac{m_1-1}{2}} \left[\frac{1}{2} + \frac{(2x-1)m_2}{2m_1}\right]} \quad (5)$$

Da m_2 zu m_1 theilerfremd ist, so kann für keinen der in Betracht kommenden Werthe von $x \frac{xm_2}{2m_1}$, beziehungsweise $\frac{(2x-1)m_2}{2m_1}$ den Bruchrest $\frac{1}{2}$ besitzen, und demnach ist

$$\left[\frac{1}{2} - \frac{xm_2}{2m_1}\right] = - \left[\frac{1}{2} + \frac{xm_2}{2m_1}\right],$$

so dass aus jeder der beiden Gleichungen die für ungerade m_0 und m_1 auch mit Hilfe des quadratischen Reciprocitätsgesetzes erweisbare Relation

$$\left(\frac{m_1}{2m_1 t_1 + m_2}\right) = \left(\frac{m_1}{2m_1 t_1 - m_2}\right)$$

folgt, in welcher als specieller Fall die Gleichung

$$\left(\frac{m_1}{m_2}\right) = \left(\frac{m_1}{-m_2}\right)$$

enthalten ist. Die Gleichungen 4) und 5) können auch in die folgende zusammengefasst werden:

$$\left(\frac{m_1}{2m_1 t_1 \pm m_2}\right) = (-1)^{\left[\frac{m_1}{2}\right] t_1} \left(\frac{m_1}{m_2}\right), \quad (6)$$

welche ein bemerkenswerthes Analogon zum bekannten Additionstheoreme der quadratischen Restcharaktere bildet. Aus derselben folgen u. A. die zwei Relationen

$$\left(\frac{m_1}{4t_1 m_1 + m_2}\right) = \left(\frac{m_1}{m_2}\right)$$

und, falls m_1 mindestens doppeltgerade, oder, wenn es ungerade ist, primär ist

$$\left(\frac{m_1}{2t_1 m_1 + m_2}\right) = \left(\frac{m_1}{m_2}\right),$$

welche auch mit Hilfe der Theorie der Gauss'schen Summen ermittelt werden können.

Ist nun

$$m_1 = g_2 m_2 + \mu_2 \quad (0 < \mu_2 < m_2),$$

so kann man auf Grund des Additionstheorems der Symbole die Gleichung 6) auch in folgender Weise schreiben

$$\left(\frac{m_1}{m_0}\right) = (-1)^{\left[\frac{m_1}{2}\right] t_1} \left(\frac{\mu_2}{m_2}\right),$$

welche Relation wegen der Gleichung

$$m_2 = 2\mu_2 t_2 \pm m_3,$$

wo m_3 wieder positiv, ungerade, kleiner als μ_2 und zu μ_2 theilerfremd ist, mit Hilfe der eben gefundenen Formel in die folgende übergeführt werden kann:

$$\left(\frac{m_1}{m_0}\right) = (-1)^{\left[\frac{m_1}{2}\right] t_1 + \left[\frac{\mu_2}{2}\right] t_2} \left(\frac{m_2}{m_3}\right).$$

Da man durch Fortsetzung dieses Verfahrens schliesslich zu einer Zahl $m_\nu = +1$ gelangen muss, so hat man den folgenden Ausdruck für den quadratischen Restcharakter:

$$\left(\frac{m_1}{m_0}\right) = (-1)^{\left[\frac{m_1}{2}\right]t_1 + \left[\frac{\mu_2}{2}\right]t_2 + \left[\frac{\mu_3}{2}\right]t_3 + \dots + \left[\frac{\mu_{\nu-1}}{2}\right]t_{\nu-1}}$$

aus welchem sich der folgende Algorithmus zur Bestimmung des Legendre-Jacobi'schen Symbols ergibt:

Leitet man aus den zwei theilerfremden ganzen Zahlen m_0 und m_1 , von denen mindestens die erste ungerade ist, in der durch das Gleichungssystem

$$m_0 = 2m_1t_1 \pm m_2$$

$$m_1 = g_2m_2 + \mu_2$$

$$m_2 = 2\mu_2t_2 \pm m_3$$

$$m_2 = g_3m_3 + \mu_3$$

$$m_3 = 2\mu_3t_3 \pm m_4$$

$$m_{\nu-1} = 2\mu_{\nu-1}t_{\nu-1} \pm 1$$

angegebenen Weise die ganzen Zahlen, $\mu_2, \mu_3, \dots, \mu_{\nu-1}; t_1, t_2, \dots, t_{\nu-1}$ ab, so hat das verallgemeinerte Legendre'sche Symbol

$\left(\frac{m_1}{m_0}\right)$ den Werth $+1$ oder -1 , je nachdem die Anzahl derjenigen

unter den Divisoren $m_1, \mu_2, \mu_3, \dots, \mu_{\nu-1}$ mit zugehörigem einfachgeraden Quotienten $2t_1, 2t_2, \dots, 2t_{\nu-1}$, welche einfach gerade oder von der Form $4s+3$ sind, gerade oder ungerade ist.

Wie rasch dieser Algorithmus oft zum Ziele führt, mag aus dem folgenden Beispiele ersehen werden. Es ist

$$1847 = 6.365 - 343$$

$$365 = 1.343 + 22$$

$$343 = 16.22 - 9$$

$$343 = 38.9 + 1$$

und demnach hat man die Gleichung

$$\left(\frac{365}{1847}\right) = +1.$$

Es sollen nun aus den Gleichungen 4) und 5) durch passende Specialisirung von m_1 , beziehungsweise m_2 , neue Relationen ermittelt werden.

Ist $m_1 = 10$, so wird die Summe im Exponenten von -1 auf der rechten Seite der Gleichung 4)

$$\sum_{x=1}^{x=0} \left[\frac{1}{2} \pm \frac{x m_2}{20} \right]$$

gleich $0, \pm 6, \pm 15, \pm 20$, je nachdem m_0 von der Form $20t \pm 1, 20t \pm 3, 20t \pm 7, 20t \pm 9$ ist, und demnach ist

$$\left(\frac{10}{m_0} \right) = (-1)^{\left[\frac{m_0}{20} + \frac{1}{2} \right]},$$

wenn m_0 die Form $20t \pm 1, 20t \pm 3$ oder $20t \pm 9$ besitzt; ist aber m_0 von der Form $20t \pm 7$, so besteht die Relation

$$\left(\frac{10}{m_0} \right) = -(-1)^{\left[\frac{m_0}{20} + \frac{1}{2} \right]}.$$

Für $m_1 = 11$ erhält die im Exponenten von -1 auf der rechten Seite der Gleichung 5) befindliche Summe

$$\sum_{x=1}^{x=5} \left[\frac{1}{2} + \frac{(2x-1)m_2}{22} \right]$$

den Werth $0, \pm 3, \pm 6, \pm 8, \pm 10$, je nachdem m_0 nach dem Modul 22 einer der Zahlen $\pm 1, \pm 3, \pm 5, \pm 7, \pm 9$ congruent ist und demnach besteht für alle ungeraden Zahlen von einer der 8 Zahlformen $22t \pm 1, 22t \pm 5, 22t \pm 7, 22t \pm 9$ die Relation

$$\left(\frac{11}{m_0} \right) = (-1)^{\left[\frac{m_0}{22} + \frac{1}{2} \right]}$$

während für $m_0 = 22t \pm 3$ die Gleichung

$$\left(\frac{11}{m_0} \right) = -(-1)^{\left[\frac{m_0}{22} + \frac{1}{2} \right]}$$

besteht.

Setzt man $m_1 = 13$, so wird der Exponent von -1 in der Gleichung 5) nach dem Modul 2 der Reihe nach den Zahlen $0, \pm 4, \pm 7, \pm 9, \pm 12, \pm 15$ congruent, wenn m_0 nach dem Modul 26, beziehungsweise $\pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 11$ congruent ist. Da nun in diesem Falle $\left[\frac{m_1}{2}\right]$ gerade ist und $\left[\frac{9m_0}{26} + \frac{1}{2}\right]$ den eben angeführten Zahlformen von m_0 entsprechend die Werthe $t_1, t_1 \pm 1, t_1 \pm 2, t_1 \pm 2, t_1 \pm 3, t_1 \pm 4$ erhält, so hat man die Gleichung

$$\left(\frac{13}{m_0}\right) = -(-1)^{\left[\frac{m_0}{26} + \frac{1}{2}\right] + \left[\frac{9m_0}{26} + \frac{1}{2}\right]}$$

Nimmt man $m_1 = 14$, so erhält die oben erwähnte Summe in der Gleichung 4) die Werthe $0, \pm 9, \pm 16, \pm 30, \pm 36, \pm 42$, je nachdem m_0 nach dem Modul 28 einer der Zahlen $\pm 1, \pm 3, \pm 5, \pm 9, \pm 11, \pm 13$ congruent ist, und daher hat man die Relationen

$$\left(\frac{14}{m_0}\right) = -(-1)^{\left[\frac{m_0}{28} + \frac{1}{2}\right]}$$

$$\left(\frac{14}{m_0}\right) = (-1)^{\left[\frac{m_0}{28} + \frac{1}{2}\right]}$$

je nachdem m_0 eine zu 7 theilerfremde ungerade Zahl von der Form $28t \pm 3$ ist oder nicht.

Ist endlich $m_1 = 17$, so ist der Werth der oben erwähnten Summe in der Gleichung 5) $0, \pm 5, \pm 9, \pm 13, \pm 16, \pm 21, \pm 24, \pm 28$, wenn m_0 nach dem Modul 34, beziehungsweise den Zahlen $\pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 11, \pm 13, \pm 15$ congruent ist.

Da in diesem Falle $\left[\frac{m_1}{2}\right]$ gerade ist und $\left[\frac{3m_0}{17} + \frac{1}{2}\right]$ den eben angeführten Formen von m_0 entsprechend die Werthe $2t_1, 2t_1 \pm 1, 2t_1 \pm 1, 2t_1 \pm 1, 2t_1 \pm 2, 2t_1 \pm 2, 2t_1 \pm 2, 2t_1 \pm 3$ erhält, so hat man die Gleichung

$$\left(\frac{17}{m_0}\right) = (-1)^{\left[\frac{3m_0}{17} + \frac{1}{2}\right]}$$

wenn m_0 eine der zwölf Formen $34t \pm 1, 34t \pm 3, 34t \pm 5, 34t \pm 7, 34t \pm 9, 34t \pm 13$ besitzt, während für $m_0 = 34t \pm 11, 34t \pm 15$ die Gleichung

$$\left(\frac{17}{m_0}\right) = -(-1)^{\left[\frac{3m_0}{17} + \frac{1}{2}\right]}$$

besteht.

Hat m_2 den Werth 1, so wird die auf der rechten Seite der Gleichung 4) im Exponenten von -1 stehende Summe

$$\sum_{x=1}^{x=m_1-1} \left[\frac{1}{2} \pm \frac{x}{2m_1} \right]$$

gleich 0 und daher hat man die Beziehung

$$\left(\frac{m_1}{m_0}\right) = \left(\frac{m_1}{2m_1 t_1 \pm 1}\right) = (-1)^{\left[\frac{m_1}{2}\right] \left[\frac{m_0}{2m_1} + \frac{1}{2}\right]},$$

welche lehrt, dass der quadratische Restcharakter von m_1 in Bezug auf $2m_1 t_1 \pm 1$ stets gleich $+1$ ist, ausser wenn m_1 von der Form $4s+3$ und die an $\frac{m_0}{2m_1}$ zunächst liegende ganze Zahl ungerade ist.

Ist $m_2 = 3$, so wird die im eben erwähnten Exponenten auftretende Summe

$$\sum_{x=1}^{x=m_1-1} \left[\frac{1}{2} \pm \frac{3x}{2m_1} \right],$$

da keines ihrer Glieder dem absoluten Betrage nach grösser als 1 sein kann und diesen Werth nur dann erhält, wenn x der Bedingung

$$m_1 > x > \frac{m_1}{3}$$

genügt, gleich $m_1 - 1 - \left[\frac{m_1}{3}\right]$ und demnach hat man die Relation

$$\left(\frac{m_1}{m_0}\right) = \left(\frac{m_1}{2m_1 t_1 \pm 3}\right) = (-1)^{\left[\frac{m_1}{2}\right] \left[\frac{m_0}{2m_1} + \frac{1}{2}\right] + m_1 - 1 - \left[\frac{m_1}{3}\right]} \quad (7)$$

so dass also speciell, wenn m_1 mehrfach gerade ist, die Gleichung

$$\left(\frac{m_1}{2m_1 t_1 \pm 3}\right) = -(-1)^{\left[\frac{m_1}{3}\right]}$$

besteht, während, falls m_1 die Form $4s+1$ besitzt,

$$\left(\frac{m_1}{2m_1t_1 \pm 3}\right) = (-1)^{\left[\frac{m_1}{3}\right]}$$

ist. Die letzte Gleichung zeigt, dass das Symbol $\left(\frac{m_1}{2m_1t_1 \pm 3}\right)$ den Werth $+1$ besitzt, wenn m_1 von der Form $12g+1$ ist, während es gleich -1 wird, wenn m_1 nach dem Modul 12 der Zahl $+5$ congruent ist. Aus der abgeleiteten Formel ersieht man

ferner, dass das Symbol $\left(\frac{m_1}{m_0}\right) = \left(\frac{m_1}{2m_1t_1 \pm 3}\right)$ den Werth

$$-(-1)^{g\left[\frac{m_0}{2m_1} + \frac{1}{2}\right]}, (-1)^{g\left[\frac{m_0}{2m_1} + \frac{1}{2}\right]}, (-1)^{(g-1)\left[\frac{m_0}{2m_1} + \frac{1}{2}\right]}$$

erhält, wenn m_1 von der Form $6g+5$, beziehungsweise $6g+1$ oder $6g+4$ beziehungsweise $6g+2$ ist.

Je nach der Beschaffenheit von m_1 kann man ferner, wie man leicht findet, die Formel 7) in einer der folgenden Weisen schreiben:

$$\left(\frac{m_1}{m_0}\right) = (-1)^{\left[\frac{m_1}{6}\right] \left[\frac{m_0}{2m_1} + \frac{1}{2}\right]} (m_1 = 6s+1)$$

$$\left(\frac{m_1}{m_0}\right) = -(-1)^{\left[\frac{m_1}{6}\right] \left[\frac{m_0}{2m_1} + \frac{1}{2}\right]} (m_1 = 6s-1)$$

$$\left(\frac{m_1}{m_0}\right) = (-1)^{\left[\frac{m_1}{6} - \frac{1}{2}\right] \left[\frac{m_0}{2m_1} + \frac{1}{2}\right]} (m_1 = 6s-2)$$

$$\left(\frac{m_1}{m_0}\right) = -(-1)^{\left[\frac{m_1}{6} - \frac{1}{2}\right] \left[\frac{m_0}{2m_1} + \frac{1}{2}\right]} (m_1 = 6s+2).$$

Nimmt man ferner $m_2 = 5$, so erhält die im Exponenten der eben angezogenen Gleichung befindliche Summe

$$\sum_{x=1}^{x=m_1-1} \left[\frac{1}{2} \pm \frac{5x}{2m_1} \right]$$

da jene von ihren Gliedern, in denen x dem Intervalle $1 \dots \frac{m_1}{5}$ angehört, gleich 0 sind, diejenigen, in denen x der Bedingung

$$\frac{3m_1}{5} > x > \frac{m_1}{5}$$

genügt, den Werth 1 besitzen, die übrigen aber gleich 2 werden.

den Werth $\left[\frac{3m_1}{5} \right] - \left[\frac{m_1}{5} \right]$ und daher hat man die Relation

$$\binom{m_1}{2m_1 t_1 \pm 5} = \left[\frac{m_1}{2} \right] \left[\frac{m_0}{2m_1} + \frac{1}{2} \right] + \left[\frac{3m_1}{5} \right] - \left[\frac{m_1}{5} \right].$$

Nun ist die Differenz $\left[\frac{3m_1}{5} \right] - \left[\frac{m_1}{5} \right]$ gerade oder ungerade, je nachdem m_1 von einer der 4 Formen $10s \pm 1$, $10s \pm 4$ oder von einer der Formen $10s \pm 3$, $10s \pm 2$ ist, und daher hat man den angeführten Zahlformen entsprechend die Relationen

$$\binom{m_1}{m_0} = \binom{m_1}{2m_1 t_1 \pm 5} = (-1)^{\left[\frac{m_1}{2} \right] \left[\frac{m_0}{2m_1} + \frac{1}{2} \right]}$$

$$\binom{m_1}{m_0} = \binom{m_1}{2m_1 t_1 \pm 5} = -(-1)^{\left[\frac{m_0}{2} \right] \left[\frac{m}{2m} + \frac{1}{2} \right]}$$

Da

$$\left[\frac{3m_1}{5} \right] - \left[\frac{m_1}{5} \right] \equiv \left[\frac{m_1}{5} \pm \frac{1}{2} \right] \pmod{2}$$

ist, je nachdem m_1 ungerade oder gerade ist, so lässt sich die eben ermittelte Formel auch in folgende zwei zerlegen:

$$\binom{m_1}{m_0} = \binom{m_1}{2m_1 t_1 \pm 5} = (-1)^{\left[\frac{m_1}{2} \right] \left[\frac{m_1}{2m_1} + \frac{1}{2} \right] + \left[\frac{m_1}{5} + \dots \right]}$$

$$\binom{m_1}{m_0} = \binom{m_1}{2m_1 t_1 \pm 5} = (-1)^{\left[\frac{m_1}{2} \right] \left[\frac{m_0}{2m_1} + \frac{1}{2} \right] + \left[\frac{m_1}{5} - \frac{1}{2} \right]},$$

von denen ich die erste a. a. O. in etwas anderer Form und auf einem weniger einfachen Wege ermittelt habe. Ich benütze diese Gelegenheit, um den daselbst im Exponenten befindlichen Druckfehler $r-1$ st. r zu verbessern.

Durch dasselbe Raisonement würde man die Gleichung

$$\binom{m_1}{m_0} = \binom{m_1}{2m_1 t_1 \pm 7} = (-1)^{\left[\frac{m_1}{2} \right] \left[\frac{m_0}{2m_1} + \frac{1}{2} \right] + m_1 - 1 + \left[\frac{m_1}{7} \right] + \left[\frac{3m_1}{7} \right] + \left[\frac{5m_1}{7} \right]}$$

ermitteln können.

Stellt man die ungerade zu m_1 theilerfremde Zahl m_0 in der Form

$$m_0 = (2t_1 + 1)m_1 \pm m_2$$

dar, wo m_1 und $m_2 < m$ theilerfremd und nach dem Modul 2 incongruent sind, so dass also

$$t_1 = \left[\frac{m_0}{2m_1} \right]$$

ist, und setzt dies in die Formeln 1) und 2) ein, so erhält man die neuen Relation

$$\begin{aligned} \left(\frac{m_1}{m_0} \right) &= \left(\frac{m_1}{(2t_1 + 1)m_1 \pm m_0} \right) = (-1)^{\left[\frac{m_1}{2} \right] \left[\frac{m_0}{2m_1} \right] + \sum_{s=1}^{s=m_1-1} \left[\frac{s+1}{2} \pm \frac{sm_2}{2m_1} \right]} \\ \left(\frac{m_1}{m_0} \right) &= (-1)^{\left[\frac{m_1}{2} \right] \left[\frac{m_0}{2m_1} \right] + \sum_{s=1}^{s=\frac{m-1}{2}} \left[\frac{(2s-1)m_2}{2m_1} \right]} \left(\frac{\pm 2}{m_1} \right) = \\ &= (-1)^{\left[\frac{m_1}{2} \right] \left[\frac{m_1}{2m_1} \right] + \sum_{s=1}^{s=\frac{m_1-1}{2}} \left[\frac{(2s-1)m_2}{2m} \right] + \left[\frac{m_1 \pm 1}{4} \right]} \end{aligned}$$

oder, da in der zweiten von ihnen $m_2 = 2\mu_2$ ist, nach einer bekannten Formel

$$\left(\frac{m_1}{m_0} \right) = (-1)^{\left[\frac{m_1}{2} \right] \left[\frac{m_0}{2m} \right]} \left(\frac{\pm m_2}{m_1} \right)$$

Vereinigt man in der im Exponenten der ersten von ihnen stehenden Summe die Glieder mit geradem x und dann jene, in denen x ungerade ist, so verwandelt sich die Relation in die folgende

$$\begin{aligned} \left(\frac{m_1}{m_0} \right) &= \left(\frac{m_1}{(2t_1 + 1)m_1 \pm m_2} \right) = \\ &= (-1)^{\left[\frac{m_1}{2} \right] \left[\frac{m_0}{2m_1} \right] + \sum_{s=1}^{s=\left[\frac{m_1-1}{2} \right]} \left[\frac{1}{2} + \frac{sm_2}{m_1} \right] + \sum_{s=1}^{s=\left[\frac{m_1}{2} \right]} \left[\pm \frac{(2s-1)m_2}{2m_1} \right]} \end{aligned}$$

Vergleicht man diese Relation mit der unmittelbar vorhergehenden, so erkennt man, dass, falls m_1 ungerade und die zu m_1 theilerfremde Zahl m_2 gerade ist, die folgende Congruenz besteht:

$$\sum_{x=1}^{\frac{m_1-1}{2}} \left[\frac{1}{2} \pm \frac{xm_2}{m_1} \right] \equiv \frac{m_1^2-1}{8} \pmod{2}.$$

Dass diese Beziehung nicht mehr besteht, wenn m_1 und m_2 einen gemeinsamen Theiler haben, zeigt schon das einfache Beispiel $m_1 = 21$, $m_2 = 6$, in welchem die Summe ± 16 , $\frac{m_1^2-1}{8}$ aber 55 ist.

Auf dem oben auseinandergesetzten Wege leitet man aus diesen allgemeinen Formeln leicht die folgenden speciellen Relationen ab:

$$\begin{aligned} \left(\frac{m_1}{(2t_1+1)m_1 \pm 2} \right) &= (-1)^{\left[\frac{m_1}{2} \right] \left[\frac{m_0}{2m_1} \right] + \left[\frac{m_1}{4} + \frac{1}{2} \right]} (\pm 1) = \\ &= (-1)^{\left[\frac{m_1}{2} \right] \left[\frac{m}{2m_1} \right] + \left[\frac{m_1 \pm 1}{4} \right]} \quad (m_1 \text{ ungerade}) \end{aligned}$$

$$\left(\frac{2m_1}{2(2t_1+1)m_1 \pm 1} \right) = (-1)^{m_1 \left[\frac{m_0}{4m_1} \right]} \cdot (\pm 1)^{m_1}$$

$$\left(\frac{m_1}{(2t_1+1)m_1 \pm 2^{\lambda} \alpha^{2\mu}} \right) = (-1)^{\left[\frac{m_1}{2} \right] \left[\frac{m_0}{2m_1} \right] + (\lambda-1) \left[\frac{m_1+1}{4} \right] + \left[\frac{m_1 \pm 1}{4} \right]} \quad (m_1, \alpha \text{ ungerade})$$

$$\left(\frac{m_1}{(2t_1+1)m_1 \pm 6} \right) = (-1)^{\left[\frac{m_1}{2} \right] \left[\frac{m_0}{2m_1} \right] + \left[\frac{m}{6} + \frac{1}{2} \right] + \left[\frac{m_1 \pm 1}{4} \right]} \quad (m_1 \text{ ungerade})$$

$$\left(\frac{m}{(2t_1+1)m_1 \pm 10} \right) = (-1)^{\left[\frac{m_1}{2} \right] \left[\frac{m_0}{2m_1} \right] + \left[\frac{m_1}{5} + \frac{1}{2} \right] + \left[\frac{m_1 \pm 1}{4} \right]} \quad (m_1 \text{ ungerade})$$

$$\left(\frac{m_1}{(2t_1+1)m_1 \pm 12} \right) = (-1)^{\left[\frac{m_1}{2} \right] \left[\frac{m_0}{2m_1} \right] + \left[\frac{m_1}{12} + \frac{1}{2} \right] + \left[\frac{m_1 \pm 1}{4} \right]} \quad (m_1 \text{ ungerade})$$

$$\left(\frac{m_1}{(2t_1+1)\pm 14}\right) = (-1)^{\left[\frac{m_1}{2}\right]\left[\frac{m_0}{2m_1}\right] + \left[\frac{m_1+1}{7}\right] + \left[\frac{m_1+1}{14}\right] + \left[\frac{m_1\pm 1}{4}\right]} \quad (m_1 \text{ ungerade})$$

$$\left(\frac{2m_1}{2(2t_1+1)m_1\pm 3}\right) = (-1)^{\left[\frac{m_1}{2}\right]\left[\frac{m_0}{2m_1}\right] + \left[\frac{m_1-1}{2}\right] + \left[\frac{m_1}{6}\right] + \frac{1\mp 1}{2}\left[\frac{m_1}{2}\right]}$$

$$\begin{aligned} \left(\frac{2m_1}{2(2t_1+1)m_1\pm 5}\right) &= \\ &= (-1)^{\left[\frac{m_1}{2}\right]\left[\frac{m_0}{2m_1} + \frac{1\mp 1}{2}\right] + \left[\frac{3m_1}{10}\right] + \left[\frac{m_1}{10}\right] + \left[\frac{m_1+1}{5}\right] + \left[\frac{2m_1+1}{5}\right]} \end{aligned}$$

$$\begin{aligned} \left(\frac{2m_1}{2(2t_1+1)m_1\pm 7}\right) &= (-1)^{\left[\frac{m_1}{2}\right]\left[\frac{m_0}{2m_1} + \frac{3\mp 1}{2}\right] + \left[\frac{m_1-1}{2}\right] + \left[\frac{m_1}{14}\right] + \left[\frac{3m_1}{14}\right]} \\ &(-1)^{\left[\frac{5m_1}{14}\right] + \left[\frac{2m_1+1}{7}\right] + \left[\frac{m_1+1}{7}\right] + \left[\frac{3m_1+1}{7}\right]} \end{aligned}$$

$$\begin{aligned} \left(\frac{2m_1}{2(2t_1+1)m_1\pm 9}\right) &= (-1)^{\left[\frac{m_1}{2}\right]\left[\frac{m_0}{2m_1} + \frac{1\mp 1}{2}\right] + \left[\frac{m_1}{18}\right] + \left[\frac{3m_1}{18}\right] + \left[\frac{5m_1}{18}\right]} \\ &(-1)^{\left[\frac{7m_1}{18}\right] + \left[\frac{m_1+1}{9}\right] + \left[\frac{2m_1+1}{9}\right] + \left[\frac{3m_1+1}{9}\right] + \left[\frac{4m_1+1}{9}\right]} \end{aligned}$$

Schreibt man die im Exponenten von -1 in der Gleichung 2a) auftretende Summe in der Form

$$\sum_{x=1}^{\frac{m_1-1}{2}} \left[\frac{xm_0}{2m_1}\right] + \sum_{x=1}^{\frac{m_1-1}{2}} \left[\frac{(m_1-x)m_0}{2m_1}\right]$$

und beachtet, dass die zweite von diesen Summen gleich

$$\frac{m_0-1}{2} \cdot \frac{m_1-1}{2} - \sum_{x=1}^{\frac{m-1}{2}} \left[\frac{xm_0}{2m_1} + \frac{1}{2}\right]$$

ist, sowie dass

$$\left[\frac{xm_0}{2m_1} + \frac{1}{2}\right] - \left[\frac{xm_0}{2m_1}\right] = \begin{cases} 0 \\ 1 \end{cases}$$

wird, je nachdem der in $\frac{xm_0}{2m_1}$ enthaltene Bruchrest kleiner oder grösser als $\frac{1}{2}$ ist, so erkennt man, dass das quadratische Reci-

prociätsgesetz die in dem folgenden Theoreme angegebene Beziehung ausspricht:

Die Anzahl der ungeraden unter den grössten ganzen Zahlen, welche in den Brüchen

$$\frac{m_0}{2m_1}, 2\frac{m_0}{2m_1}, 3\frac{m_0}{2m_1}, \dots, (m_1-1)\frac{m_0}{2m_1}$$

enthalten sind, ist nach dem Modul 2 der Anzahl derjenigen in der ersten Hälfte enthaltenen Brüche, deren Bruchrest grösser als $\frac{1}{2}$ ist, congruent oder nicht, je nachdem mindestens eine oder keine der beiden theilerfremden Zahlen m_0, m_1 von der Form $4s+1$ ist.

Zum Schlusse will ich bei dieser Gelegenheit noch folgende zwei leicht zu beweisende Sätze angeben:

Ist τ die Anzahl der Transformationen einer Form der Fundamentaldiscriminante Δ in sich selbst, $\varphi(\Delta, n)$ die Anzahl der Darstellungen der ganzen Zahl n durch das System der quadratischen Formen der genannten Discriminante

$$Y(x) - Z(x) i^{\frac{1}{2}(\Delta-1)} \sqrt{\Delta} = 2 \left[a \right] (x - e^{\frac{2a\pi i}{\Delta}})$$

$$Y(x) + Z(x) i^{\frac{1}{2}(\Delta-1)} \sqrt{\Delta} = 2 \left[b \right] (x - e^{\frac{2b\pi i}{\Delta}})$$

wo das erste auf a bezügliche Product über alle zu Δ theilerfremden Zahlen unterhalb Δ erstreckt wird, für welche das Legendre-Jacobi'sche Symbol $\left(\frac{a}{\Delta}\right) = +1$ ist, das auf b bezügliche aber über alle von ihnen, für welche $\left(\frac{b}{\Delta}\right) = -1$ ist, so hat man für alle x , die dem absoluten Betrage noch kleiner als 1 sind, die Beziehung

$$\left(\frac{Y(x) - Z(x)(\sqrt{\Delta})}{Y(x) + Z(x)(\sqrt{\Delta})} \right) = \prod_{n=1}^{\infty} (1 - x^n)^{\frac{(\sqrt{\Delta})\varphi(\Delta, n)}{n}}$$

wo $(\sqrt{\Delta})$ der Hauptwerth von $\sqrt{\Delta}$ ist.

Addirt man zu allen Gliedern eines vollständigen Restensystems für den ungeraden Modul m mit Ausschluss der Null eine Zahl α , so besitzen unter den dadurch entstehenden Zahlen $r-1$, denselben (quadratischen, beziehungsweise cubischen beziehungsweise biquadratischen) Charakter, wie die Zahl α , es gehören zu jeder Gruppe eines von α verschiedenen Charakters r , und es ist endlich eine durch den Modul theilbar, wo r für quadratische Reste $\frac{m-1}{2}$ für cubische $\frac{\text{Norm } m-1}{3}$ für biquadratische $\frac{\text{Norm } m-1}{4}$ ist.

Dieses Theorem enthält als speciellen Fall einen in Legendre's „Théorie des nombres“ aufgestellten Satz.

ZOBODAT - www.zobodat.at

Zoologisch-Botanische Datenbank/Zoological-Botanical Database

Digitale Literatur/Digital Literature

Zeitschrift/Journal: [Sitzungsberichte der Akademie der Wissenschaften mathematisch-naturwissenschaftliche Klasse](#)

Jahr/Year: 1891

Band/Volume: [100_2a](#)

Autor(en)/Author(s): Gegenbauer Leopold

Artikel/Article: [Über den quadratischen Restcharakter. 1072-1087](#)