Kongruenzen zwischen Koeffizienten trigonometrischer Reihen und Klassenzahlen quadratisch imaginärer Körper.

Kongruenzen zwischen Koeffizienten trigonometrischer Reihen und Klassenzahlen quadratisch imaginärer Körper

von M. GUT und M. STÜNZI (Zürich)

Prof. ROLF NEVANLINNA gewidmet

Inhaltsangabe und Bezeichnungen

Beziehungen von der im Titel erwähnten Art finden sich schon bei *Cauchy* [2] und in einer Arbeit von *Adolf Hurwitz* [5].

Es sei $d < -4$ die Diskriminante eines quadratisch imaginären Körpers mit der Klassenzahl $h(d) = h$. Es sei ferner p eine ungerade Primzahl und $d = -mp$, wo die natürliche Zahl m auch gleich 1 sein darf. Dann zeigen wir in der vorliegenden Arbeit, dass wenn man die von *Ankeny, Artin und Chowla* [1] eingeführten trigonometrischen Reihen

$$\frac{1}{e^{mx}-1}\sum_{t=1}^{m} X(t)e^{tx} = \sum_{n=-1}^{\infty} C((-1)^{(p+1)/2}m\,;\,n)\frac{x^n}{n!} \tag{1}$$

benutzt, sich das im Vergleich zu den Sätzen in der Arbeit von *Adolf Hurwitz* [5] überraschend einfache Resultat

$$-h \equiv C((-1)^{(p+1)/2}m\,;\,(p-1)/2) \pmod{p} \tag{2}$$

ergibt. Dabei bedeutet $X(n)$ für jede natürliche Zahl n den Charakter mod. m:

$$X(n) = \left(\frac{(-1)^{(p+1)/2}m}{n}\right), \quad \text{sodass} \quad \left(\frac{d}{n}\right) = X(n)\left(\frac{(-1)^{(p-1)/2}p}{n}\right) = X(n)\left(\frac{n}{p}\right). \tag{3}$$

Wir bemerken noch, dass wenn $m \neq 1$ ist, auf der linken Seite der Formel (1) die Summation über t auch nur von 1 bis $m-1$ erstreckt werden kann und auf der rechten Seite die Summation über n nur von 0 bis ∞.

Ausgehend von der Klassenzahlformel

$$-h\,|d| = \sum_{n=1}^{|d|-1} n\left(\frac{d}{n}\right), \quad d < -4, \tag{4}$$

geben wir im folgenden den Beweis durch sukzessive Betrachtung folgender Fälle:

1. Hauptfall $d \equiv 0 \pmod{4}$, $d \neq -4$

In diesem Falle ist in $d = -mp$ die natürliche Zahl m durch 4 teilbar. Wir zeigen zuerst, dass wenn die Argumente natürliche Zahlen sind

$$X(n) = -X(n + m/2). \tag{1.1}$$

Zum Beweise betrachten wir die beiden Unterfälle:

1. Unterfall: $d = 4D$, wo $D \equiv 3 \pmod{4}$, $d \neq -4$

Setzt man in $d = -mp$ die natürliche Zahl $m = 4m'$, so ist m' eine quadratfreie und zu p teilerfremde natürliche Zahl. Da $\frac{d}{4} = -m'p \equiv 3 \pmod{4}$ ist, ist $m'p \equiv 1 \pmod{4}$, also

$$m' \equiv (-1)^{(p-1)/2} \pmod{4}.$$

Ist n eine *ungerade* natürliche Zahl, so ist erstens

$$X(n) = \left(\frac{(-1)^{(p+1)/2} m}{n}\right) = \left(\frac{(-1)^{(p+1)/2} m'}{n}\right).$$

Da der Zähler im letzten Ausdruck $\equiv -1 \pmod{4}$ und der Nenner positiv ist, folgt nach dem allgemeinen quadratischen Reziprozitätsgesetz

$$X(n) = \left(\frac{n}{m'}\right)(-1)^{(n-1)/2}.$$

Zweitens wird analog, da m' ungerade ist

$$X(n + m/2) = X(n + 2m') = \left(\frac{(-1)^{(p+1)/2} m}{n + 2m'}\right) = \left(\frac{(-1)^{(p+1)/2} m'}{n + 2m'}\right)$$
$$= \left(\frac{n + 2m'}{m'}\right)(-1)^{(n+2m'-1)/2} = -\left(\frac{n}{m'}\right)(-1)^{(n-1)/2}.$$

Mithin gilt die Gleichung (1.1) für ungerade natürliche Zahlen n. Sie gilt aber auch für gerade natürliche Zahlen, denn dann verschwinden beide Seiten der Gleichung.

2. Unterfall: $d = 4D$, wo $D \equiv 2 \pmod{4}$

Setzt man in $d = -mp$ die natürliche Zahl $m = 8m'$, so ist m' eine quadratfreie und zu p teilerfremde ungerade natürliche Zahl.

Ist n eine *ungerade* natürliche Zahl, so ist erstens

$$X(n) = \left(\frac{(-1)^{(p+1)/2} m}{n}\right) = \left(\frac{(-1)^{(p+1)/2} 2m'}{n}\right) = \left(\frac{2}{n}\right)\left(\frac{-1}{n}\right)^{(p+1)/2}\left(\frac{m'}{n}\right).$$

Da n positiv ist, folgt nach dem allgemeinen quadratischen Reziprozitätsgesetz:

$$X(n) = (-1)^{\frac{n^2-1}{8}} \cdot (-1)^{\frac{n-1}{2} \cdot \frac{p+1}{2}} \cdot (-1)^{\frac{n-1}{2} \cdot \frac{m'-1}{2}} \left(\frac{n}{m'}\right).$$

Zweitens wird

$$\begin{aligned} X(n+m/2) &= X(n+4m') = \left(\frac{(-1)^{(p+1)/2} m}{n+4m'}\right) = \left(\frac{(-1)^{(p+1)/2} 2\, m'}{n+4m'}\right) \\ &= \left(\frac{2}{n+4m'}\right)\left(\frac{-1}{n+4m'}\right)^{(p+1)/2} \left(\frac{m'}{n+4m'}\right) \\ &= (-1)^{\frac{(n+4m')^2-1}{8}} \cdot (-1)^{\frac{n+4m'-1}{2} \cdot \frac{p+1}{2}} \cdot (-1)^{\frac{n+4m'-1}{2} \cdot \frac{m'-1}{2}} \left(\frac{n+4m'}{m'}\right). \end{aligned}$$

Reduziert man die Exponenten mod. 2, so folgt, da nm' ungerade ist

$$\begin{aligned} X\left(n+\frac{m}{2}\right) &= (-1)^{\frac{n^2-1}{8}} \cdot (-1)^{nm'} \cdot (-1)^{\frac{n-1}{2} \cdot \frac{p+1}{2}} \cdot (-1)^{\frac{n-1}{2} \cdot \frac{m'-1}{2}} \cdot \left(\frac{n}{m'}\right) \\ &= -(-1)^{\frac{n^2-1}{8}} \cdot (-1)^{\frac{n-1}{2} \cdot \frac{p+1}{2}} \cdot (-1)^{\frac{n-1}{2} \cdot \frac{m'-1}{2}} \left(\frac{n}{m'}\right). \end{aligned}$$

Folglich gilt (1.1) für ungerade natürliche Zahlen n; wie schon beim 1. Unterfall gilt sie aber auch für gerade natürliche Zahlen n, denn dann verschwinden beide Seiten der Gleichung.

Im folgenden brauchen wir diese Fallunterscheidung nicht mehr, d.h. es sei von nun an nur vorausgesetzt, dass $d \equiv 0 \pmod{4}$, $d < -4$ ist.

Da p ungerade und $X(n)$ für positive n ein Charakter mod. m ist, folgt aus (1.1):

$$X(n) = -X(n+mp/2). \tag{1.2}$$

Für die Klassenzahl $h = h(d)$ ergibt sich mithin

$$-h\,|d| = \sum_{n=1}^{|d|-1} n\left(\frac{d}{n}\right) = \sum_{n=1}^{mp-1} n\,X(n)\left(\frac{n}{p}\right),$$

also da $mp/2$ gerade ist

$$= \sum_{n=1}^{mp/2-1} n\,X(n)\left(\frac{n}{p}\right) + \sum_{n^*=mp/2+1}^{mp-1} n^* X(n^*)\left(\frac{n^*}{p}\right).$$

Setzt man in der 2. Summe $n^* = n + mp/2$, so folgt aus (1.2):

$$- hmp = \sum_{n=1}^{mp/2-1} n X(n) \left(\frac{n}{p}\right) - \sum_{n=1}^{mp/2-1} (n + mp/2) X(n) \left(\frac{n}{p}\right) =$$

$$= - \frac{mp}{2} \sum_{n=1}^{mp/2-1} X(n) \left(\frac{n}{p}\right).$$

Daher wird

$$2h = \sum_{n=1}^{mp/2-1} X(n) \left(\frac{n}{p}\right). \tag{1.3}$$

Modulo p wird mithin

$$2\left(\frac{2}{p}\right) h = \sum_{n=1}^{mp/2-1} X(n) \left(\frac{2n}{p}\right) \equiv \sum_{n=1}^{mp/2-1} X(n)(2n)^{(p-1)/2} \quad (\mathrm{mod.}\, p), \tag{1.4}$$

$$\left.\begin{array}{l} \text{also } 2\left(\frac{2}{p}\right) h \text{ mod. } p \text{ kongruent dem Koeffizienten von} \\ \qquad \dfrac{x^{(p-1)/2}}{\frac{p-1}{2}!} \quad \text{in} \quad \displaystyle\sum_{n=1}^{mp/2-1} X(n) \exp 2nx. \end{array}\right\} \tag{1.5}$$

Die zuletzt aufgeführte Summe und auch jede Summe, für welche für *jede* feste Potenz von x bis zur (p-1)-ten Potenz inklusive der Koeffizient mod. p kongruent ist dem Koeffizienten der gleichen festen Potenz von x in *dieser* Summe, wollen wir mit $S(x)$ bezeichnen. Wir fassen in $S(x)$ die Glieder zusammen, die modulo m kongruenten Werten von n entsprechen:

$$S(x) = \sum_{n=1}^{mp/2-1} X(n) \exp 2nx = \sum_{t=1}^{m-1} X(t) \sum_{k} \exp 2(t + km)x. \tag{1.6}$$

Für den Exponenten $2(t+km)x$ gilt:

$$0 < t + km < mp/2, \tag{1.7}$$

also

$$0 < t/m + k < p/2$$

oder

$$- t/m < k < p/2 - t/m = (p-1)/2 + (1/2 - t/m).$$

Mithin durchläuft k die Werte

$$\left.\begin{array}{lll} k = 0, 1, 2, \ldots, (p-3)/2, (p-1)/2 & \text{für} & t < m/2 \\ k = 0, 1, 2, \ldots, (p-3)/2 & \text{für} & t > m/2 \end{array}\right\} \tag{1.8}$$

Es ist also

$$S(x) = \sum_{t=1}^{m/2-1} X(t)[\exp 2tx + \exp(2t+2m)x + \cdots + \exp(2t+(p-1)m)x] +$$

$$+ \sum_{t=m/2+1}^{m-1} X(t)[\exp 2tx + \exp(2t+2m)x + \cdots + \exp(2t+(p-3)m)x],$$

mithin

$$S(x) = \sum_{t=1}^{m/2-1} X(t)\,(\exp 2tx)\,\frac{(\exp(p+1)mx)-1}{(\exp 2mx)-1} +$$

$$+ \sum_{t=m/2+1}^{m-1} X(t)\,(\exp 2tx)\,\frac{(\exp(p-1)mx)-1}{(\exp 2mx)-1}.$$

Nehmen wir die Exponenten sinngemäss nach (1.5) mod. p, so folgt:

$$S(x) = \sum_{t=1}^{m/2-1} X(t)\,(\exp 2tx)\,\frac{(\exp mx)-1}{(\exp 2mx)-1} +$$

$$+ \sum_{t^*=m/2+1}^{m-1} X(t^*)\,(\exp 2t^*x)\,\frac{(\exp -mx)-1}{(\exp 2mx)-1}.$$

Setzt man in der 2. Summe $t^* = t + m/2$, so erhält man unter Berücksichtigung von (1.1):

$$S(x) = \sum_{t=1}^{m/2-1} X(t)\,(\exp 2tx)\,\frac{(\exp mx)-1}{(\exp 2mx)-1} -$$

$$- \sum_{t=1}^{m/2-1} X(t)\,(\exp 2tx)\,\frac{1-\exp mx}{(\exp 2mx)-1}.$$

Mithin ist

$$S(x) = 2\sum_{t=1}^{m/2-1} X(t)\,(\exp 2tx)\,\frac{(\exp mx)-1}{(\exp 2mx)-1}.$$

Da $X(n)$ für positive n ein Charakter mod. m ist, folgt:

$$S(x) = -2 \sum_{t=1}^{m/2-1} X(t) \frac{\exp 2tx}{(\exp 2mx)-1} + 2 \sum_{t^*=1}^{m/2-1} X(t^*+m) \cdot \frac{\exp (2t^*+m)x}{(\exp 2mx)-1}.$$

Setzt man $t^*+m/2=t$ so ergibt sich vermöge (1.1):

$$S(x) = -2 \sum_{t=1}^{m/2-1} X(t) \frac{\exp 2tx}{(\exp 2mx)-1} - 2 \sum_{t=m/2+1}^{m-1} X(t) \frac{\exp 2tx}{(\exp 2mx)-1},$$

also gemäss (1):

$$S(x) = -2 \sum_{t=1}^{m-1} X(t) \frac{\exp 2tx}{(\exp 2mx)-1} = -2 \sum_{n=-1}^{\infty} C((-1)^{(p+1)/2}m;\, n) \frac{2^n x^n}{n!}.$$

Aus den Formeln (1.4) und (1.5) folgt:

$$2\left(\frac{2}{p}\right) h \equiv -2 \cdot 2^{(p-1)/2} C\left((-1)^{(p+1)/2}m;\, \frac{p-1}{2}\right) \quad (\text{mod.}\, p)$$

und daher die zu beweisende Kongruenz (2):

$$-h \equiv C\left((-1)^{(p+1)/2}m;\, \frac{p-1}{2}\right) \quad (\text{mod.}\, p).$$

Bemerkung: Für jede nicht negative ganze Zahl n ist $C(-4;\, n) = -E_n/2$, wo E_n die n-te *Euler*sche Zahl ist.

2. Hauptfall $d \equiv 1$ (mod. 4), $d \neq -3$. Erster Teil

Aus (4) folgt:

$$-h\,|d| = \sum_{n=1}^{(|d|-1)/2} n \left(\frac{d}{n}\right) + \sum_{n^*=(|d|+1)/2}^{|d|-1} n^* \left(\frac{d}{n^*}\right).$$

Setzt man in der 2. Summe $n^* = |d| - n$, so folgt, da gemäss *Hecke* [4], Satz 137, pg. 187 für natürliche Zahlen n und m

$$\left(\frac{d}{n}\right) = \left(\frac{d}{m}\right) \text{sign}\, d, \text{ falls } n \equiv -m \quad (\text{mod.}\, |d|), \tag{2.1}$$

dass

$$-h|d| = 2 \sum_{n=1}^{(|d|-1)/2} n\left(\frac{d}{n}\right) - |d| \sum_{n=1}^{(|d|-1)/2} \left(\frac{d}{n}\right). \tag{2.2}$$

Anderseits folgt aus (4), falls man je die Summanden gleicher Parität zusammenfasst:

$$-h|d| = \sum_{n=1}^{(|d|-1)/2} 2n\left(\frac{d}{2n}\right) + \sum_{\substack{n^*=1 \\ n^* \equiv 1 \ (\mathrm{mod.}\ 2)}}^{|d|-2} n^*\left(\frac{d}{n^*}\right).$$

Setzt man in der 2. Summe $n^* = |d| - n'$ und hernach $n' = 2n$, so folgt:

$$-h|d| = 2\left(\frac{d}{2}\right) \sum_{n=1}^{(|d|-1)/2} n\left(\frac{d}{n}\right) - \sum_{n=1}^{(|d|-1)/2} (|d| - 2n)\left(\frac{d}{2n}\right).$$

Multipliziert man beide Seiten dieser Gleichung mit $\left(\frac{d}{2}\right)$, so ergibt sich

$$-h|d|\left(\frac{d}{2}\right) = 4 \sum_{n=1}^{(|d|-1)/2} n\left(\frac{d}{n}\right) - |d| \sum_{n=1}^{(|d|-1)/2} \left(\frac{d}{n}\right). \tag{2.3}$$

Multipliziert man beide Seiten von (2.2) mit -2 und addiert zum Ergebnis Seite für Seite die Gleichung (2.3), teilt ferner beide Seiten des Resultates durch $|d|$, so erhält man schliesslich:

$$h\left[2 - \left(\frac{d}{2}\right)\right] = \sum_{n=1}^{(|d|-1)/2} \left(\frac{d}{n}\right). \tag{2.4}$$

Gemäss Formel (3) folgt aus (2.4):

$$h\left[2 - X(2)\left(\frac{2}{p}\right)\right] = \sum_{n=1}^{(mp-1)/2} X(n)\left(\frac{n}{p}\right). \tag{2.5}$$

Multipliziert man beide Seiten dieser Gleichung mit $\left(\frac{2}{p}\right)$, so folgt:

$$h\left[2\left(\frac{2}{p}\right) - X(2)\right] = \sum_{n=1}^{(mp-1)/2} X(n)\left(\frac{2n}{p}\right). \tag{2.6}$$

Modulo p gilt mithin:

$$h\left[2\left(\frac{2}{p}\right)-X(2)\right] \equiv \sum_{n=1}^{(mp-1)/2} X(n)(2n)^{(p-1)/2} \pmod{p} \tag{2.7}$$

$$\left.\begin{array}{l} \text{also } h\left[2\left(\frac{2}{p}\right)-X(2)\right] \text{ mod. } p \text{ kongruent dem Koeffizienten von} \\ \dfrac{x^{(p-1)/2}}{((p-1)/2)!} \quad \text{in} \quad \displaystyle\sum_{n=1}^{(mp-1)/2} X(n) \exp 2nx \end{array}\right\} \tag{2.8}$$

Wiederholt man mutatis mutandis die Überlegungen, die auf die Relation (1.5) folgen, so ergibt sich

$$S(x) = \sum_{n=1}^{(mp-1)/2} X(n) \exp 2nx = \sum_{t=1}^{m} X(t) \sum_{k} \exp 2(t+km)x. \tag{2.9}$$

Für den Exponenten $2(t+km)x$ gilt

$$0 < t + km < mp/2.$$

Diese Ungleichungen sind aber die gleichen wie (1.7). Mithin gelten für k auch die Ungleichungen (1.8). Es ist also

$$S(x) = \sum_{t=1}^{(m-1)/2} X(t)[\exp 2tx + \exp(2t+2m)x + \cdots + \exp(2t+(p-1)m)x] +$$

$$+ \sum_{t=(m+1)/2}^{m} X(t)[\exp 2tx + \exp(2t+2m)x + \cdots + \exp(2t+(p-3)m)x].$$

Dabei hat es natürlich hier und in folgenden analogen Summationen die Meinung dass wenn $m=1$ ist, der erste der beiden Summanden der rechten Seite identisch verschwindet. Es folgt:

$$S(x) = \sum_{t=1}^{(m-1)/2} X(t)(\exp 2tx) \frac{(\exp(p+1)mx)-1}{(\exp 2mx)-1} +$$

$$+ \sum_{t=(m+1)/2}^{m} X(t)(\exp 2tx) \frac{(\exp(p-1)mx)-1}{(\exp 2mx)-1}.$$

Nehmen wir die Exponenten sinngemäss nach (2.8) mod. p, so folgt:

$$S(x)=\sum_{t=1}^{(m-1)/2} X(t)\,(\exp 2tx)\,\frac{(\exp mx)-1}{(\exp 2mx)-1}+$$
$$+\sum_{t=(m+1)/2}^{m} X(t)\,(\exp 2tx)\,\frac{(\exp(-mx))-1}{(\exp 2mx)-1}.$$

Mithin ist

für $m=1$:

$$S(x)=(\exp 2x)\,\frac{(\exp -x)-1}{(\exp 2x)-1}. \tag{2.10}$$

für $m>1$:

$$S(x)=-\sum_{t=1}^{m-1} X(t)\,\frac{\exp 2tx}{(\exp 2mx)-1}+\sum_{t=1}^{(m-1)/2} X(t)\,(\exp 2tx)\,\frac{\exp mx}{(\exp 2mx)-1}+$$
$$+\sum_{t=(m+1)/2}^{m-1} X(t)\,(\exp 2tx)\,\frac{\exp(-mx)}{(\exp 2mx)-1}. \tag{2.11}$$

Wir führen zuerst den Beweis zu Ende für den Fall, dass $m=1$ ist. Gemäss (2.10) wird

$$S(x)=\frac{\exp x-\exp 2x}{(\exp 2x)-1}=\frac{(\exp x)(1+\exp x)-2\exp 2x}{(\exp 2x)-1}=$$
$$=\frac{\exp x}{(\exp x)-1}-2\,\frac{\exp 2x}{(\exp 2x)-1}.$$

Wenn $m=1$, also $d=-p$ ist, ist $p\equiv 3 \pmod 4$ und nach Voraussetzung $d\neq -3$, also $p\neq 3$. Für $m=1$ gibt die Formel (1) daher

$$S(x)=\sum_{n=-1}^{\infty} C(1;n)\,\frac{x^n}{n!}-2\sum_{n=-1}^{\infty} C(1;n)\,\frac{(2x)^n}{n!}.$$

Gemäss (3) ist $X(2)=(\frac{1}{2})=1$ und daher gemäss (2.8)

$$h\left[2\left(\frac{2}{p}\right)-1\right]\equiv C(1;(p-1)/2)-2\left(\frac{2}{p}\right)C(1;(p-1)/2) \quad (\mathrm{mod.}\,p),$$

also
$$-h\left[2\left(\frac{2}{p}\right)-1\right]\equiv\left[2\left(\frac{2}{p}\right)-1\right]C(1;(p-1)/2)\quad(\mathrm{mod.}\,p).$$
Da die eckige Klammer zu p teilerfremd ist, ergibt sich
$$-h\equiv C(1;(p-1)/2)\quad(\mathrm{mod.}\,p),$$
womit (2) bewiesen ist.

Bemerkung: Für jede natürliche Zahl n ist $C(1;n-1)=B_n/n$, wo B_n die n-te *Bernoullische* Zahl ist.

In der Folge sei also immer $m>1$. Gemäss (2.11) ist dann
$$S(x)=-2\sum_{t=1}^{m-1}X(t)\frac{\exp 2tx}{(\exp 2mx)-1}+\sum_{t=1}^{(m-1)/2}X(t)(\exp 2tx)\frac{(\exp mx)+1}{(\exp 2mx)-1}+$$
$$+\sum_{t=(m+1)/2}^{m-1}X(t)(\exp 2tx)\frac{(\exp -mx)+1}{(\exp 2mx)-1}.$$
Da das Quadrat von $X(2)$ gleich 1 und für positive Argumente $X(2t)=X(2t-m)$ ist, folgt:
$$S(x)=-2\sum_{t=1}^{m-1}X(t)\frac{\exp 2tx}{(\exp 2mx)-1}+X(2)\sum_{t^*=1}^{(m-1)/2}X(2t^*)\frac{\exp(2t^*x)}{(\exp mx)-1}+$$
$$+X(2)\sum_{t^*=(m+1)/2}^{m-1}X(2t^*-m)\frac{\exp(2t^*-m)x}{(\exp mx)-1}.$$
Setzt man in der vorletzten Summe $2t^*=t$ und in der letzten Summe $2t^*-m=t$, so ergibt sich
$$S(x)=-2\sum_{t=1}^{m-1}X(t)\cdot\frac{\exp 2tx}{(\exp 2mx)-1}+X(2)\sum_{\substack{t=2\\t\equiv 0\,(\mathrm{mod.}\,2)}}^{m-1}X(t)\cdot\frac{\exp tx}{(\exp mx)-1}+$$
$$+X(2)\sum_{\substack{t=1\\t\equiv 1\,(\mathrm{mod.}\,2)}}^{m-2}X(t)\cdot\frac{\exp tx}{(\exp mx)-1},$$
also
$$S(x)=-2\sum_{t=1}^{m-1}X(t)\cdot\frac{\exp 2tx}{(\exp 2mx)-1}+X(2)\sum_{t=1}^{m-1}X(t)\cdot\frac{\exp tx}{(\exp mx)-1}.$$

Nach Formel (1) ergibt sich, da $X(m)=0$ ist

$$S(x)=-2\sum_{n=-1}^{\infty} C((-1)^{(p+1)/2}m\,;\,n)\frac{(2x)^n}{n!}+X(2)\sum_{n=-1}^{\infty} C((-1)^{(p+1)/2}m\,;\,n)\frac{x^n}{n!}.$$

Daher ist gemäss der Formel (2.8):

$$h\left[2\left(\frac{2}{p}\right)-X(2)\right]\equiv\left[X(2)-2\left(\frac{2}{p}\right)\right]C((-1)^{(p+1)/2}m\,;\,(p-1)/2)\quad(\mathrm{mod.}\,p).$$

Für den Fall, dass die eckige Klammer zu p teilerfremd ist, wird

$$-h\equiv C((-1)^{(p+1)/2}m\,;\,(p-1)/2)\quad(\mathrm{mod.}\,p),$$

womit (2) bewiesen ist.
Die eckige Klammer ist aber genau dann und nur dann zu p teilerfremd, wenn $p=3$ und gleichzeitig $X(2)=\left(\frac{2}{p}\right)=(\frac{2}{3})=-1$ oder wenn $p\neq 3$ ist.
Es ist also (2) nur noch zu beweisen für den Fall, dass $p=3$ und gleichzeitig $X(2)=1$, also $\left(\frac{d}{2}\right)=-1$ ist. Dies sei in der Folge immer angenommen.

2. Hauptfall $d\equiv 1$ (mod. 4), $d\neq -3$. Zweiter Teil

Da $d=-3m\equiv 1$ (mod. 4) ist, ist $m\equiv 1$ (mod. 4) und wegen $X(2)=1$ sogar $m\equiv 1$ (mod. 8). Ferner ist $X(n)$ jetzt gleich $\left(\frac{m}{n}\right)$, folglich $X(n)=X(m-n)$, falls beide Argumente natürliche Zahlen sind. Endlich ist $m\equiv 1$ (mod. 3) oder $m\equiv 2$ (mod. 3) und $m\neq 1$.

Wir setzen zur Abkürzung

$$\left.\begin{aligned} A&=\sum_{n^*=1}^{(m-1)/2} X(n^*)\left(\frac{n^*}{3}\right),\\ D&=\sum_{n^*=(m+1)/2}^{m-1} X(n^*)\left(\frac{n^*}{3}\right),\\ G&=\sum_{n^*=m+1}^{(3m-1)/2} X(n^*)\left(\frac{n^*}{3}\right).\end{aligned}\right\}\tag{3.1}$$

Dann ist also nach Formel (2.5)

$$3h=A+D+G.\tag{3.2}$$

Aus dieser Gleichung gewinnen wir in drei Schritten eine Gleichung, in der h selbst durch eine Summe von ganzen Zahlen ausgedrückt wird.

Wir setzen in A den Summationsbuchstaben $n^* = n$,
in D den Summationsbuchstaben $n^* = m - n$
und in G den Summationsbuchstaben $n^* = m + n$.

Es wird, weil $-1 = \left(\frac{-1}{3}\right)$ ist:

$$A - D + G = \sum_{n=1}^{(m-1)/2} X(n) \left\{ \left(\frac{n}{3}\right) + \left(\frac{n-m}{3}\right) + \left(\frac{n+m}{3}\right) \right\}.$$

Da die geschweifte Klammer für jeden Wert von n immer verschwindet, ist $A + G = D$, also gemäss (3.2):

$$D = 3h/2. \tag{3.3}$$

Wir zeigen nun, dass

$$A = 0 \tag{3.4}$$

ist.

Ist erstens $m \equiv 1 \pmod{3}$, so ist

$$A = \sum_{\substack{n^*=1 \\ n^* \equiv 1 \,(\mathrm{mod.}\, 3)}}^{(m-5)/2} X(n^*) - \sum_{\substack{n^*=2 \\ n^* \equiv 2 \,(\mathrm{mod.}\, 3)}}^{(m-3)/2} X(n^*).$$

Da $X(2) = 1$ ist, folgt

$$A = \sum_{\substack{n^*=1 \\ n^* \equiv 1 \,(\mathrm{mod.}\, 3)}}^{(m-5)/2} X(4n^*) - \sum_{\substack{n^*=2 \\ n^* \equiv 2 \,(\mathrm{mod.}\, 3)}}^{(m-3)/2} X(2n^*).$$

Es wird mithin, falls man in der ersten Summe $4n^* = n$ setzt und in der zweiten Summe $2n^* = n$:

$$A = \sum_{\substack{n=4 \\ n \equiv 4 \,(\mathrm{mod.}\, 12)}}^{2m-10} X(n) - \sum_{\substack{n=4 \\ n \equiv 4 \,(\mathrm{mod.}\, 6)}}^{m-3} X(n).$$

Unterteilt man jede der beiden Summen in zwei Summanden, so folgt:

$$A = \sum_{\substack{n=4 \\ n \equiv 4 \,(\mathrm{mod.}\, 12)}}^{m-9} X(n) + \sum_{\substack{n=m+3 \\ n \equiv 4 \,(\mathrm{mod.}\, 12)}}^{2m-10} X(n) - \sum_{\substack{n=4 \\ n \equiv 4 \,(\mathrm{mod.}\, 12)}}^{m-9} X(n) - \sum_{\substack{n^*=10 \\ n^* \equiv 10 \,(\mathrm{mod.}\, 12)}}^{m-3} X(n^*).$$

Die Summe des ersten und dritten Summanden verschwindet. Ebenso verschwindet die Summe des zweiten und vierten Summanden, wie man sofort sieht, wenn man in der letzten Summe $n^* = 2m - n$ setzt.

Ist zweitens $m \equiv 2 \pmod{3}$, also

$$A = \sum_{\substack{n^*=1 \\ n^* \equiv 1 \,(\mathrm{mod.}\, 3)}}^{(m-3)/2} X(n^*) - \sum_{\substack{n^*=2 \\ n^* \equiv 2 \,(\mathrm{mod.}\, 3)}}^{(m-1)/2} X(n^*),$$

so folgt analog:

$$A = \sum_{\substack{n^*=1 \\ n^* \equiv 1 \ (\mathrm{mod.}\ 3)}}^{(m-3)/2} X(2n^*) - \sum_{\substack{n^*=2 \\ n^* \equiv 2 \ (\mathrm{mod.}\ 3)}}^{(m-1)/2} X(4n^*),$$

also

$$A = \sum_{\substack{n=2 \\ n \equiv 2 (\mathrm{\ mod.}\ 6)}}^{m-3} X(n) \quad - \sum_{\substack{n=8 \\ n \equiv 8 \ (\mathrm{mod.}\ 12)}}^{2m-2} X(n).$$

Unterteilt man wieder jeden der beiden Summanden, so ergibt sich:

$$A = \sum_{\substack{n=2 \\ n \equiv 2 \ (\mathrm{mod.}\ 12)}}^{m-3} X(n) + \sum_{\substack{n=8 \\ n \equiv 8 \ (\mathrm{mod.}\ 12)}}^{m-9} X(n) - \sum_{\substack{n=8 \\ n \equiv 8 \ (\mathrm{mod.}\ 12)}}^{m-9} X(n) - \sum_{\substack{n^*=m+3 \\ n^* \equiv 8 \ (\mathrm{mod.}\ 12)}}^{2m-2} X(n^*).$$

Die Summe des zweiten und dritten Summanden verschwindet. Ebenso verschwindet die Summe des ersten und vierten Summanden, wie man sofort sieht, wenn man in der letzten Summe wieder $n^* = 2m - n$ setzt.

Damit ist (3.4) bewiesen.

Geht man aus von den beiden Formeln (3.3) und (3.4) und setzt man in der zweiten der Formeln (3.1) den Summationsbuchstaben $n^* = m - n$, beachtet schliesslich noch, dass $\sum_{n=1}^{(m-1)/2} X(n) = 0$ ist, so erhält man

$$3h/2 = D = D + A = \sum_{n=1}^{(m-1)/2} X(n) \left\{ \left(\frac{m-n}{3} \right) + \left(\frac{n}{3} \right) - \left(\frac{m}{3} \right) \right\}.$$

Ist daher

$$\left.\begin{aligned} \mu &= 1, \quad \text{wenn} \quad m \equiv 1 \quad (\mathrm{mod.}\ 3) \\ \mu &= 2, \quad \text{wenn} \quad m \equiv 2 \quad (\mathrm{mod.}\ 3) \end{aligned}\right\} \tag{3.5}$$

so ergibt sich

$$3h/2 = -3X(3) \sum_{\substack{n=3-\mu \\ n \equiv -m \ (\mathrm{mod.}\ 3)}}^{(m-3)/2} X(n)$$

und mithin

$$h/2 = -X(3) \sum_{\substack{n^*=3-\mu \\ n^* \equiv -m \ (\mathrm{mod.}\ 3)}}^{(m-3)/2} X(n^*).$$

Zum Schlusse befreien wir uns noch von der Kongruenzvorschrift über den Summanden. Beachtet man, dass $X(n^*) = X(n^* + m)$ ist, setzt man $n^* + m = n'$ und hierauf

$n'=3n$, so erhält man

$$h/2 = -X(3) \sum_{\substack{n^*=3-\mu \\ n^*\equiv -m\,(\mathrm{mod.}\,3)}}^{(m-3)/2} X(n^*+m) = -X(3) \sum_{\substack{n'=3+m-\mu \\ n'\equiv 0\,(\mathrm{mod.}\,3)}}^{(3m-3)/2} X(n') =$$

$$= -X(3) \sum_{n=1+(m-\mu)/3}^{(m-1)/2} X(3n),$$

also

$$h/2 = -\sum_{n=1+(m-\mu)/3}^{(m-1)/2} X(n).$$

Addiert man Seite für Seite die Gleichung:

$$0 = \sum_{n=1}^{(m-\mu)/3} X(n) + \sum_{n=1+(m-\mu)/3}^{(m-1)/2} X(n),$$

so ergibt sich

$$h = 2\sum_{n=1}^{(m-\mu)/3} X(n). \tag{3.6}$$

Die Gleichung (3.6) gibt also den genauen Wert für h und ist natürlich wertvoller als die Kongruenz (2), die wir jetzt zum Schluss noch beweisen werden.

Es sei, vgl. (1)

$$f(x) = \frac{1}{(\exp mx)-1} \sum_{t=1}^{m-1} X(t) \exp tx = \sum_{n=0}^{\infty} C(m;n)\frac{x^n}{n!}.$$

Da $f(-x) = -f(x)$, mithin $f(x)$ eine ungerade Funktion ist, ist $C(m;0)=0$. Folglich wird

$$C(m;1) = \lim_{x\to 0}\frac{f(x)}{x} = \lim_{x\to 0}\frac{\sum_{t=1}^{m-1} X(t)\exp tx}{x((\exp mx)-1)}.$$

Da Zähler und Nenner für $x=0$ verschwinden, wird

$$C(m;1) = \lim_{x\to 0}\frac{\sum_{t=1}^{m-1} tX(t)\exp tx}{(1+mx)(\exp mx)-1}.$$

Hier verschwinden für $x=0$ nochmals sowohl der Zähler wie der Nenner. Daher wird

$$C(m;1) = \lim_{x\to 0}\frac{\sum_{t=1}^{m-1} t^2 X(t)\exp tx}{(2m+xm^2)\exp mx},$$

d.h.

$$C(m;1)=\frac{1}{2m}\sum_{t=1}^{m-1} t^2 X(t). \tag{3.7}$$

Weil $\sum_{t=1}^{m-1} X(t)=0$ ist, ist

$$C(m;1)=\frac{1}{2m}\sum_{t=1}^{m-1}\{t^2-1\}X(t).$$

Mithin wird modulo 3:

$$C(m;1)\equiv-\frac{1}{2m}\sum_{\substack{t=3\\ t\equiv 0\,(\mathrm{mod.}\,3)}}^{m-\mu} X(t) \quad (\mathrm{mod.}\ 3).$$

Setzt man $t=3n$ und beachtet, dass $X(3)=\left(\frac{m}{3}\right)\equiv m$ (mod. 3) ist, so ergibt sich

$$C(m;1)\equiv\sum_{n=1}^{(m-\mu)/3} X(n) \quad (\mathrm{mod.}\ 3) \tag{3.8}$$

Aus (3.6) und (3.8) folgt:

$$-h\equiv C(m;1) \quad (\mathrm{mod.}\ 3). \tag{3.9}$$

Die Kongruenz (3.9) ist aber wegen $p=3$ und $(p-1)/2=1$ die zu beweisende Kongruenz (2).

Bemerkung

Da $h\geqq 1$ ist, so ist klar, dass wenn $h\leqq p$ ist, der kleinste ganzzahlige positive Rest mod. p von $-C\left((-1)^{\frac{p+1}{2}}m;\frac{p-1}{2}\right)$ gleich der Klassenzahl $h=h(d)$ selbst ist.

Nun gelten jedenfalls folgende beiden Sätze, vgl. *Gut* [3]:

Es liege ein imaginär quadratischer Zahlkörper mit der Diskriminanten d vor, so dass für ganzrationalzahliges quadratfreies D:

entweder $d=D$, $D\equiv 1$ (mod. 4)

oder $d=4D, D\equiv 2{,}3$ (mod. 4).

Ist k der Körper der rationalen Zahlen, so ist also der Körper mit der Diskriminanten d der Körper $k(\sqrt{D})$.

HAUPTSATZ. Für die Klassenzahl h des Körpers $k(\sqrt{D})$, wo $d<-4$ ist, gilt die Ungleichung

$$h<|d|/4.$$

ZUSATZ. Wenn $d=4D$, $D\equiv 2{,}3 \pmod 4$ ist, gilt sogar die Ungleichung

$$h < |d|/12 = |D|/3,$$

falls man, abgesehen von dem sowieso ausgeschlossenen Fall $d=-4$, die Körper mit den Diskriminanten $d=-8$, $d=-20$ und $d=-24$ ausschliesst.

Für alle Diskriminanten $d<-4$ ist also insbesondere der kleinste ganzzahlige positive Rest mod. p von $-C\left((-1)^{\frac{p+1}{2}}m;\frac{p-1}{2}\right)$ für *jede* ungerade Primzahl p immer die Klassenzahl selbst, wenn $d\equiv 1 \pmod 4$ und $m=1$ oder $m=3$ ist, bezw., wenn $d\equiv 0 \pmod 4$ und $m\leqq 12$ ist.

LITERATURVERZEICHNIS

[1] N. C. ANKENY, E. ARTIN UND S. CHOWLA, The class-number of real quadratic number fields, Ann. Math. 56 (1952), 479–493.

[2] A. L. CAUCHY, Mémoire sur la théorie des nombres. Mémoires de l'Académie royale des sciences de l'Institut de France, t. 17 (1840). Oeuvres, (I), *3*, 5–452.

[3] M. GUT, Abschätzungen für die Klassenzahlen der quadratischen Körper. Acta Arithmetica VIII (1963), 113–122.

[4] E. HECKE, Vorlesungen über die Theorie der algebraischen Zahlen, Leipzig 1923.

[5] A. HURWITZ, Ueber die Anzahl der Klassen binärer quadratischer Formen von negativer Determinante. Math. Werke Bd. II S. 208 und Acta Mathematica Bd. *19* (1895), 351 und *20* (1897), 312.

Eingegangen den 7. Mai 1966

Zusatz bei der Korrektur:

Wie ich nachträglich von den Herren A. A. KISELEV und J. Sch. SLAVUTSKY erfahren habe, enthält eine 1964 in Leningrad erschienene von ihnen verfasste Arbeit (Trudy Četvertogo Vsesojuznogo Matematičeskogo Sezda, 3.–12. Juli 1961, Bd. II, S. 105–112, Leningrad 1964) nicht nur die Formel (2), sondern für h auch Kongruenzen modulo einer *Potenz* von p für gewisse Koeffizienten von grösserem als dem Index $(p\text{-}1)/2$ der Reihe auf der rechten Seite von (1). Ihr Resultat ist natürlich mit anderen Mitteln als dem hier benutzten Eulerschen Kriterium gewonnen worden. [M.G.]