

ÜBER DIE ANZAHL DER CLASSEN BINÄRER QUADRATISCHER FORMEN  
VON NEGATIVER DETERMINANTE

VON

A. HURWITZ  
in ZÜRICH.

1.

In der vorliegenden Abhandlung bezeichnet der Buchstabe  $P$  stets eine positive ungerade ganze Zahl, die grösser als 1 ist und ausser durch 1 durch keine Quadratzahl theilbar ist. Ferner bedeutet  $h(D)$  die Anzahl der Classen, in welche die eigentlich primitiven positiven Formen

$$ax^2 + 2bxy + cy^2$$

der negativen Determinante

$$b^2 - ac = -D$$

zerfallen. Wenn zur Abkürzung der Schreibweise

$$\frac{1}{8}P = \omega$$

gesetzt wird, so bestehen nach DIRICHLET<sup>1</sup> die folgenden Gleichungen, welche die Classenzahlen durch Summen von Legendre-Jacobischen Zeichen darstellen:

---

<sup>1</sup> *Vorlesungen über Zahlentheorie* (herausgegeben von R. DEDEKIND) § 106.  
*Acta mathematica*. 19. Imprimé le 9 juillet 1895.

$$\begin{aligned}
 \text{I.} \quad h(P) &= \sum_0^{4\omega} \left(\frac{s}{P}\right), & \text{falls } P \equiv 3 \pmod{4}, \\
 \text{II.} \quad h(P) &= 2 \sum_0^{2\omega} \left(\frac{s}{P}\right), & \text{falls } P \equiv 1 \pmod{4}, \\
 \text{III.} \quad h(2P) &= 2 \sum_\omega^{3\omega} \left(\frac{s}{P}\right), & \text{falls } P \equiv 3 \pmod{4}, \\
 \text{IV.} \quad h(2P) &= 2 \left\{ \sum_0^\omega \left(\frac{s}{P}\right) - \sum_{3\omega}^{4\omega} \left(\frac{s}{P}\right) \right\}, & \text{falls } P \equiv 1 \pmod{4}.
 \end{aligned}$$

Unter dem Zeichen

$$\sum_m^n f(s)$$

ist hier, wie stets in der Folge, die Summe derjenigen Werthe der Function  $f$  zu verstehen, welche den im Intervalle  $m \dots n$  liegenden ganzzahligen Argumenten  $s$  entsprechen, so dass sich also die Summation auf alle ganzen Zahlen  $s$  erstreckt, welche die Ungleichungen

$$m \leq s \leq n$$

erfüllen.

Da jedes Legendre-Jacobische Zeichen einen der Werthe  $0, 1, -1$  besitzt, so leuchtet ein, dass die Classenzahlen  $h(P)$  und  $h(2P)$  einen unterhalb  $\frac{1}{2}P$ , also umsomehr unter  $P$  liegenden Werth besitzen. Kennt man daher eine Zahl, welcher  $h(P)$  oder  $h(2P)$  nach dem Modul  $P$  congruent ist, so ist die Classenzahl  $h(P)$  oder  $h(2P)$  als der kleinste positive Rest jener Zahl modulo  $P$  eindeutig bestimmt. Von dieser Bemerkung ausgehend, bin ich zu einer Reihe von Sätzen gelangt, die ich im Folgenden entwickeln will. Zur Orientirung über die Natur dieser Sätze, will ich hier zunächst die einfachsten derselben, die sich auf den Fall beziehen, wo  $P$  eine Primzahl ist, angeben.

**1. Satz.** Die Entwicklung von  $\operatorname{tg} x$  nach Potenzen von  $x$  laute:

$$\operatorname{tg} x = \alpha_1 x + \alpha_2 \frac{x^3}{3} + \alpha_3 \frac{x^5}{5} + \dots + \alpha_n \frac{x^{2n-1}}{(2n-1)} + \dots$$

Über die Anzahl der Classen binärer quadratischer Formen von negativer Determinante. 353

Wenn nun  $p$  irgend eine Primzahl von der Form  $4n + 3$  bezeichnet, so ist die Classenzahl  $h(p)$  der kleinste positive Rest von

$$(-1)^{\frac{p+1}{4}} \frac{1}{2} \alpha_{\frac{p+1}{4}}$$

nach dem Modul  $p$ .

Beispielsweise ist die Classenzahl  $h(11)$  bestimmt durch die Congruenz

$$h(11) \equiv -\frac{1}{2} \alpha_3 \pmod{11}$$

und hat also, da  $\alpha_3 = 16$  ist, den Werth 3.

**2. Satz.** Die Entwicklung von  $\frac{1}{\cos x}$  nach Potenzen von  $x$  laute:

$$\frac{1}{\cos x} = \beta_0 + \beta_1 \frac{x^2}{2} + \beta_2 \frac{x^4}{4} + \dots + \beta_n \frac{x^{2n}}{(2n)} + \dots$$

Wenn nun  $p$  irgend eine Primzahl von der Form  $4n + 1$  bezeichnet, so ist die Classenzahl  $h(p)$  der kleinste positive Rest von

$$(-1)^{\frac{p-1}{4}} \frac{1}{2} \beta_{\frac{p-1}{4}}$$

nach dem Modul  $p$ .

Zum Beispiel ist hiernach

$$h(17) \equiv \frac{1}{2} \beta_4 \pmod{17}$$

und also  $h(17) = 4$ , da  $\beta_4 = 1385$  ist.

**3. Satz.** Die Entwicklung von  $\frac{\sin x}{\cos 2x}$  nach Potenzen von  $x$  laute:

$$\frac{\sin x}{\cos 2x} = r_1 x + r_2 \frac{x^3}{3} + r_3 \frac{x^5}{5} + \dots + r_n \frac{x^{2n-1}}{(2n-1)} + \dots$$

Wenn nun  $p$  irgend eine Primzahl von der Form  $4n + 3$  bezeichnet, so ist die Classenzahl  $h(2p)$  der kleinste positive Rest von

$$(-1)^{\frac{p+1}{4}} \cdot r_{\frac{p+1}{4}}$$

nach dem Modul  $p$ .

Beispiel:  $h(22) \equiv -\gamma_3 \equiv -361 \pmod{11}$ , also  $h(22) = 2$ .

4. Satz. Die Entwicklung von  $\frac{\cos x}{\cos 2x}$  nach Potenzen von  $x$  laute:

$$\frac{\cos x}{\cos 2x} = \delta_0 + \delta_1 \frac{x^2}{2} + \delta_2 \frac{x^4}{4} + \dots + \delta_n \frac{x^{2n}}{(2n)} + \dots$$

Wenn nun  $p$  irgend eine Primzahl von der Form  $4n + 1$  bezeichnet, so ist die Classenzahl  $h(2p)$  der kleinste positive Rest von

$$(-1)^{\frac{p-1}{4}} \cdot \delta_{\frac{p-1}{4}}$$

nach dem Modul  $p$ .

Beispiel:  $h(26) \equiv -\delta_3 \equiv -2763 \pmod{13}$ , also  $h(26) = 6$ .

Um den Gang der Untersuchung später nicht unterbrechen zu müssen, knüpfe ich an diese Sätze gleich hier einige Bemerkungen:

Die Tangentkoeffizienten  $\alpha_1, \alpha_2, \dots$  stehen bekanntlich zu den Bernoullischen Zahlen  $B_1, B_2, \dots$  in der Beziehung

$$\alpha_n = \frac{2^{2n}(2^{2n} - 1)}{2n} B_n.$$

Daher ist

$$\frac{1}{2} \alpha_{\frac{p+1}{4}} \equiv 2^{\frac{p+1}{2}} \left( 2^{\frac{p+1}{2}} - 1 \right) B_{\frac{p+1}{4}} \equiv 2 \left( 2^p - 2^{\frac{p-1}{2}} \right) B_{\frac{p+1}{4}} \equiv 2 \left( 2 - \left( \frac{2}{p} \right) \right) B_{\frac{p+1}{4}} \pmod{p}.$$

Der Satz 1. kann hiernach auch dahin ausgesprochen werden, dass die Classenzahl  $h(p)$  durch die Congruenz bestimmt ist

$$h(p) \equiv -6 B_{\frac{p+1}{4}} \pmod{p},$$

wenn  $p$  eine Primzahl von der Form  $8n + 3$  und durch die Congruenz

$$h(p) \equiv 2 B_{\frac{p+1}{4}} \pmod{p},$$

wenn  $p$  eine Primzahl von der Form  $8n + 7$  ist.

Bei dieser Formulierung des Satzes ist aber der Fall  $p = 3$  auszuschliessen, was darin seinen Grund hat, dass für diesen (und nur für diesen) Fall  $B_{\frac{p+1}{4}}$  einen durch  $p$  theilbaren Nenner besitzt.

Die Coefficienten  $\beta_0, \beta_1, \dots$  sind die sogenannten Euler'schen Zahlen. Bekanntlich sind diese, ebenso wie die Tangentencoefficienten  $\alpha_1, \alpha_2, \dots$ , *positive ganze Zahlen*. Das Gleiche gilt aber, wie ich jetzt zeigen will, auch für die Entwicklungscoefficienten  $\gamma_1, \gamma_2, \dots$  und  $\delta_0, \delta_1, \dots$ .

Dass diese Entwicklungscoefficienten *ganze Zahlen* sind, ergibt sich unmittelbar aus den Recursionsformeln, welche man für dieselben aus den identischen Gleichungen:

$$\frac{\sin x}{\cos 2x} \cos 2x = \sin x, \quad \frac{\cos x}{\cos 2x} \cos 2x = \cos x$$

erhält. Um zu beweisen, dass dieselben *positive Zahlen* sind, zerlege ich

$$\frac{\cos x + \sin x}{\cos 2x} = \frac{1}{\sqrt{2}} \frac{1}{\cos\left(x + \frac{\pi}{2}\right)}$$

in Partialbrüche:

$$\frac{\cos x + \sin x}{\cos 2x} = -\frac{1}{\sqrt{2}} \sum_1^{\infty} k \frac{(-1)^{\frac{k(k+1)}{2}}}{(2k-1)\frac{\pi}{4} + (-1)^k x},$$

wobei die Glieder der Summe nach wachsenden Werthen von  $k$  anzuordnen sind. Entwickelt man die einzelnen Glieder nach aufsteigenden Potenzen von  $x$  und vergleicht die Coefficienten von  $x^n$  auf beiden Seiten der vorstehenden Gleichung, so ergibt sich:

$$\gamma_n = \left\{ (2n-1) \left(\frac{4}{\pi}\right)^{2n} \frac{1}{\sqrt{2}} \left[ 1 - \frac{1}{3^{2n}} - \frac{1}{5^{2n}} + \frac{1}{7^{2n}} + \frac{1}{9^{2n}} - \dots \right] \right\},$$

$$\delta_n = \left\{ (2n) \left(\frac{4}{\pi}\right)^{2n+1} \frac{1}{\sqrt{2}} \left[ 1 + \frac{1}{3^{2n+1}} - \frac{1}{5^{2n+1}} - \frac{1}{7^{2n+1}} + \frac{1}{9^{2n+1}} - \dots \right] \right\}.$$

Aus diesen Darstellungen der Zahlen  $\gamma_n, \delta_n$  geht nun hervor, dass dieselben *positive* Werthe besitzen. Denn die Differenzen  $1 - \frac{1}{3^{2n}} - \frac{1}{5^{2n}}$ ,  $\frac{1}{7^{2n}} - \frac{1}{9^{2n}}$ ,  $\frac{1}{11^{2n}} - \frac{1}{13^{2n}}$ ,  $\dots$ , ebenso wie  $1 - \frac{1}{5^{2n+1}}$ ,  $\frac{1}{3^{2n+1}} - \frac{1}{7^{2n+1}}$ ,  $\dots$  sind sämmtlich positiv.

## 2.

Zur Abkürzung der Beweise für die oben angegebenen Sätze und für andere Sätze ähnlichen Charakters, benutze ich den Begriff der Congruenz in einem erweiterten Umfange. Einerseits dehne ich den Begriff der Congruenz, wie dies auch sonst seit GAUSS hin und wieder geschieht, auf rationale Zahlen aus. Zwei rationale Zahlen  $r$  und  $s$  mögen nämlich nach dem ganzzahligen Modul  $m$  congruent heissen, in Zeichen

$$(1) \quad r \equiv s \pmod{m},$$

wenn ihre Differenz  $r - s$ , auf die kleinste Benennung gebracht, einen durch  $m$  theilbaren Zähler besitzt. Dass derartige Congruenzen addirt und subtrahirt werden dürfen, d. h. dass aus der Congruenz (1) und der Congruenz

$$(2) \quad r' \equiv s' \pmod{m}$$

die neuen Congruenzen

$$r \pm r' \equiv s \pm s' \pmod{m}$$

folgen, leuchtet unmittelbar ein.

Um die Gesetze für die Multiplication und Division solcher Congruenzen leicht aussprechen zu können, ist es zweckmässig noch folgende Definitionen einzuführen:

Eine rationale Zahl heisse *endlich* nach dem Modul  $m$ , wenn sie, auf die kleinste Benennung gebracht, einen zu  $m$  theilerfremden Nenner besitzt.

Eine rationale Zahl heisse *relativ prim* zum Modul  $m$ , wenn sie selbst und zugleich ihr reciproker Werth endlich nach dem Modul  $m$  ist.

Eine rationale Zahl, die man auf die kleinste Benennung gebracht hat, ist offenbar stets und nur dann relativ prim zu  $m$ , wenn sowohl ihr Zähler wie ihr Nenner theilerfremd zu  $m$  ist.

Man zeigt ferner leicht, dass zwei nach dem Modul  $m$  congruente rationale Zahlen gleichzeitig endlich modulo  $m$  oder nicht und gleichzeitig relativ prim zu  $m$  oder nicht sind.

Was nun die Gesetze der Multiplication und Division für die hier betrachteten Congruenzen angeht, so sind dieselben in folgenden Sätzen enthalten, deren Beweise ich übergehe, da sie ganz elementarer Natur sind.

»Besteht die Congruenz (1), so bleibt dieselbe richtig, wenn ihre Glieder  $r$  und  $s$  mit irgend einer (mod.  $m$ ) endlichen Zahl multiplicirt werden.»

»Aus den Congruenz (1) und (2) darf man die Congruenz

$$rr' \equiv ss' \pmod{m}$$

folgern, wenn  $r$  und  $r'$  endlich nach dem Modul  $m$  sind.»

»Die Congruenz (1) zieht die Congruenz

$$\frac{r'}{r} \equiv \frac{s'}{s} \pmod{m}$$

nach sich, wenn  $r$  relativ prim zu  $m$  ist.»

»Aus den Congruenzen (1) und (2) darf man die Congruenz

$$\frac{r'}{r} \equiv \frac{s'}{s} \pmod{m}$$

folgern, wenn  $r'$  endlich und  $r$  relativ prim zum Modul  $m$  ist.»

Eine andere Erweiterung des Congruenzbegriffes, die ich im Folgenden benutze, bezieht sich auf Potenzreihen mit rationalen Coefficienten. Es seien

$$(3) \quad \varphi(x) = r_0 + r_1x + r_2 \frac{x^2}{2} + \dots + r_n \frac{x^n}{n} + \dots,$$

$$(4) \quad \psi(x) = s_0 + s_1x + s_2 \frac{x^2}{2} + \dots + s_n \frac{x^n}{n} + \dots$$

zwei Potenzreihen, die in der Umgebung der Stelle  $x = 0$  convergiren und rationale Coefficienten besitzen. Die Congruenz

$$(5) \quad \varphi(x) \equiv \psi(x) \pmod{m}$$

soll dann nichts anderes ausdrücken, als dass für jeden Index  $n$

$$(6) \quad r_n \equiv s_n \pmod{m}$$

ist. Ferner will ich sagen, die Congruenz (5) bestehe bis zu den Gliedern  $k^{\text{ter}}$  Ordnung, wenn die Congruenz (6) für  $n = 0, 1, 2, \dots, k$  erfüllt ist.

Die Potenzreihe (3)  $\varphi(x)$  möge *endlich* heissen nach dem Modul  $m$ , wenn alle Coefficienten  $r_0, r_1, r_2, \dots$  endlich sind nach dem Modul  $m$ .

Ist  $\varphi(x)$  endlich nach dem Modul  $m$  und zugleich das Anfangsglied  $r_0$  relativ prim zu  $m$ , so soll  $\varphi(x)$  selbst *relativ prim* zu  $m$  heissen.

An diese Begriffe knüpfen sich nun die folgenden Sätze:

1.) »Ist  $\varphi(x)$  relativ prim zu  $m$ , so ist auch  $\frac{1}{\varphi(x)}$  relativ prim zu  $m$ .«

Denn ist  $\frac{1}{\varphi(x)} = r'_0 + r'_1 x + r'_2 \frac{x^2}{2} + \dots$ , so hat man

$$\begin{aligned} r'_0 r_0 &= 1, & r'_1 r_0 + r'_0 r_1 &= 0, & r'_2 r_0 + 2r'_1 r_1 + r'_0 r_2 &= 0, \\ & & r'_3 r_0 + 3r'_2 r_1 + 3r'_1 r_2 + r'_0 r_3 &= 0, & \dots \end{aligned}$$

Berechnet man aus diesen Gleichungen  $r'_0, r'_1, r'_2, \dots$ , so erkennt man, dass diese Zahlen sämtlich endlich und die erste  $r'_0$  überdies relativ prim zum Modul  $m$  sind.

Fasst man dieselben Gleichungen als Congruenzen (mod.  $m$ ) auf, so ergibt sich leicht der Satz:

2.) »Ist  $\varphi(x)$  relativ prim zu  $m$  und  $\varphi(x) \cdot \varphi_1(x) \equiv 1 \pmod{m}$ , so ist  $\varphi_1(x) \equiv \frac{1}{\varphi(x)} \pmod{m}$ .«

Sind  $r$  und  $s$  nach dem Modul  $m$  congruente und endliche Zahlen, so sind auch  $r^n$  und  $s^n$  congruent und endlich für jeden positiven ganzzahligen Exponenten  $n$ . Daraus folgt:

3.) »Sind  $r$  und  $s$  nach dem Modul  $m$  congruente und endliche Zahlen, so ist

$$\varphi(rx) \equiv \varphi(sx) \pmod{m}$$

wenn  $\varphi(x)$  nach dem Modul  $m$  endlich ist.«

Zwischen den Potenzreihen (3) und (4) möge jetzt die Congruenz (5) bestehen. Ferner sei

$$(7) \quad \chi(x) = t_0 + t_1 \frac{x}{1} + t_2 \frac{x^2}{2} + \dots + t_n \frac{x^n}{n} + \dots$$

eine (mod.  $m$ ) endliche Potenzreihe. Ein Blick auf die Gleichungen



$$(8) \begin{cases} \varphi(x)\chi(x) = r_0 t_0 + (r_1 t_0 + r_0 t_1) \frac{x}{1} + (r_2 t_0 + 2r_1 t_1 + r_0 t_2) \frac{x^2}{2} + \dots, \\ \psi(x)\chi(x) = s_0 t_0 + (s_1 t_0 + s_0 t_1) \frac{x}{1} + (s_2 t_0 + 2s_1 t_1 + s_0 t_2) \frac{x^2}{2} + \dots \end{cases}$$

lehrt dann, dass die Potenzreihen  $\varphi(x)\chi(x)$  und  $\psi(x)\chi(x) \pmod{m}$  congruent sind. Es besteht also der Satz:

4.) »Ist  $\varphi(x) \equiv \psi(x) \pmod{m}$  und  $\chi(x)$  endlich nach dem Modul  $m$ , so ist auch  $\varphi(x)\chi(x) \equiv \psi(x)\chi(x) \pmod{m}$ .

Combinirt man hiermit den Satz 1.), so erhält man

5.) »Ist  $\varphi(x) \equiv \psi(x) \pmod{m}$  und  $\chi(x)$  relativ prim zu  $m$ , so ist auch  $\frac{\varphi(x)}{\chi(x)} \equiv \frac{\psi(x)}{\chi(x)} \pmod{m}$ ».

Sind  $\varphi(x)$  und  $\psi(x)$  congruent  $\pmod{m}$  und relativ prim zu  $m$ , bezeichnen ferner für einen Augenblick  $\varphi_1(x)$  und  $\psi_1(x)$  die Potenzreihen  $\frac{1}{\varphi(x)}$  bez.  $\frac{1}{\psi(x)}$ , so folgt aus  $\varphi(x) \equiv \psi(x) \pmod{m}$  nach Satz 4.)

$$1 \equiv \varphi(x)\varphi_1(x) \equiv \psi(x)\psi_1(x) \pmod{m}$$

und hieraus nach Satz 2.)  $\varphi_1(x) \equiv \psi_1(x) \pmod{m}$ . D. h.

6.) »Ist  $\varphi(x) \equiv \psi(x) \pmod{m}$  und  $\varphi(x)$  relativ prim zu  $m$ , so ist auch  $\frac{1}{\varphi(x)} \equiv \frac{1}{\psi(x)} \pmod{m}$ ».

Es seien jetzt  $\varphi(x)$ ,  $\psi(x)$ ,  $\varphi_1(x)$ ,  $\psi_1(x)$  irgend vier Potenzreihen mit rationalen Coefficienten und

$$(9) \begin{cases} \varphi(x) \equiv \psi(x) \pmod{m}, \\ \varphi_1(x) \equiv \psi_1(x) \pmod{m} \end{cases}$$

Dann gelten für die Combination dieser Congruenzen durch Addition, Subtraction, Multiplication und Division folgende Gesetze:

7.) Aus den Congruenzen (9) darf man folgern

a) die Congruenzen  $\varphi(x) \pm \varphi_1(x) \equiv \psi(x) \pm \psi_1(x) \pmod{m}$  ohne jede Einschränkung;

b) die Congruenz  $\varphi(x)\varphi_1(x) \equiv \psi(x)\psi_1(x) \pmod{m}$ , wenn  $\varphi(x)$  und  $\varphi_1(x)$  endlich sind modulo  $m$ ;

c) die Congruenz  $\frac{\varphi_1(x)}{\varphi(x)} \equiv \frac{\psi_1(x)}{\psi(x)} \pmod{m}$ , wenn  $\varphi_1(x)$  endlich  $\pmod{m}$  und  $\varphi(x)$  relativ prim zu  $m$  ist.

Schliesslich habe ich noch einen in der Folge wiederholt zur Anwendung gelangenden Satz zu entwickeln, der sich auf die Frage bezieht, in wie weit eine Congruenz  $\varphi(x) \equiv \psi(x) \pmod{m}$  durch eine mit  $x$  verschwindende Potenzreihe  $\chi(x)$  dividierbar ist. Ich nehme an, dass  $\chi(x)$  von der ersten Ordnung verschwindet, dass also

$$\chi(x) = t_1 x + t_2 \frac{x^2}{2} + t_3 \frac{x^3}{3} + \dots$$

ist, wo  $t_1$  von Null verschieden. Ferner setze ich voraus, dass  $\varphi(x)$  und  $\psi(x)$  für  $x = 0$  verschwinden, also  $r_0$  und  $s_0$  in den Entwicklungen (3) und (4) Null sind. Ist nun

$$\frac{\varphi(x)}{\chi(x)} = \varphi_1(x) = r'_0 + r'_1 x + r'_2 \frac{x^2}{2} + \dots,$$

$$\frac{\psi(x)}{\chi(x)} = \psi_1(x) = s'_0 + s'_1 x + s'_2 \frac{x^2}{2} + \dots,$$

so folgt aus der Annahme  $\varphi(x) \equiv \psi(x)$ , oder  $\varphi_1(x)\chi(x) \equiv \psi_1(x)\chi(x) \pmod{m}$ , dass die Zahlen

$$r'_0 t_1, 2r'_1 t_1 + r'_0 t_2, 3r'_2 t_1 + 3r'_1 t_2 + r'_0 t_3, \dots$$

der Reihe nach  $\pmod{m}$  congruent sind den Zahlen

$$s'_0 t_1, 2s'_1 t_1 + s'_0 t_2, 3s'_2 t_1 + 3s'_1 t_2 + s'_0 t_3, \dots$$

Hieraus ergibt sich successive  $r'_0 \equiv s'_0, r'_1 \equiv s'_1, \dots, r'_{p-1} \equiv s'_{p-1} \pmod{m}$  unter der Annahme, dass  $t_1, 2t_1, 3t_1, \dots, (p-1)t_1$  relativ prim zu  $m$  und  $t_2, t_3, \dots, t_p$  endlich nach dem Modul  $m$  sind. Die erstere Annahme ist erfüllt, wenn  $t_1$  relativ prim zu  $m$  und  $p$  die kleinste in  $m$  aufgehende Primzahl ist. Hiernach kann man folgenden Satz aussprechen:

8.) »Sind  $\varphi(x)$  und  $\psi(x)$  mit  $x$  verschwindende Potenzreihen und ist

$$\chi(x) = t_1 x + t_2 \frac{x^2}{2} + t_3 \frac{x^3}{3} + \dots$$

endlich nach dem Modul  $m$ , während zugleich  $t_1$  relativ prim zu  $m$  ist, so folgt aus dem Bestehen der Congruenz

$$\varphi(x) \equiv \psi(x) \pmod{m},$$

dass die Congruenz

$$\frac{\varphi(x)}{\chi(x)} \equiv \frac{\psi(x)}{\chi(x)} \pmod{m}$$

bis zu den Gliedern  $(p - 1)^{\text{ter}}$  Ordnung gilt, unter  $p$  die kleinste in  $m$  aufgehende Primzahl verstanden.»

### 3.

Ehe ich zu dem eigentlichen Gegenstande dieser Abhandlung übergehe, will ich die Sätze der vorigen Nummer an einigen Beispielen erläutern.

Nach dem Modul 3 bestehen (Satz 3.) der vorigen Nummer) die Congruenzen

$$\cos 3x \equiv 1, \quad \cos 2x \equiv \cos(-x) \equiv \cos x \pmod{3}.$$

Die elementare Gleichung  $\cos x(2 \cos 2x - 1) = \cos 3x$ , ergibt daher die Congruenz

$$\cos x(2 \cos x - 1) \equiv 1 \pmod{3}.$$

Also ist (nach Satz 2. oder 5. der vorigen Nummer)

$$(1) \quad \frac{1}{\cos x} \equiv 2 \cos x - 1 \equiv -(1 + \cos x) \pmod{3}.$$

Der Coefficient von  $\frac{x^{2n}}{(2n)!}$  auf der linken Seite dieser Congruenz ist die Euler'sche Zahl  $\beta_n$ , auf der rechten Seite ist derselbe  $(-1)^{n+1}$ . Man erhält also den bekannten Satz, nach welchem die Euler'sche Zahl  $\beta_n$  von der Form  $3k - 1$  oder  $3k + 1$  ist, je nachdem  $n$  gerade oder ungerade ist.

In ähnlicher Weise ergibt sich die Congruenz

$$(2) \quad \frac{1}{\cos x} \equiv 1 + 2 \cos x - 2 \cos 2x \pmod{5},$$

welche den Satz enthält, dass die Euler'sche Zahl  $\beta_n \equiv 1$  oder  $0 \pmod{5}$  ist, je nachdem  $n$  ungerade oder gerade ist. Aus der Congruenz

$$\sin x \cos x = \frac{1}{2} \sin 2x \equiv x \pmod{4}$$

folgt

$$\frac{x}{\cos x} \equiv \sin x \pmod{4}.$$

Da der Coefficient von  $\frac{x^{2n+1}}{2n+1}$  auf der linken Seite

$$(2n+1)\beta_n \equiv (-1)^n \beta_n \pmod{4},$$

auf der rechten Seite  $(-1)^n$  ist, so besagt diese Congruenz, dass die Euler'schen Zahlen sämmtlich  $\equiv 1 \pmod{4}$  sind.

Multipliziert man die vorstehenden Congruenzen (1) und (2) mit  $\sin x$ , so erhält man

$$\frac{\sin x}{\cos x} \equiv - \left( \sin x + \frac{1}{2} \sin 2x \right) \equiv - (\sin x + \sin x) \equiv \sin x \pmod{3},$$

$$\frac{\sin x}{\cos x} \equiv \sin x + \sin 2x - \sin 3x + \sin x \equiv 2(\sin x + \sin 2x) \pmod{5}.$$

D. h. der Tangentencoefficient  $\alpha_n$  ist  $\equiv 1$  oder  $2$  nach den Moduln  $3$  und  $5$  (und also nach dem Modul  $15$ ) je nachdem  $n$  ungerade oder gerade ist. Um den Rest von  $\alpha_n \pmod{8}$  zu beurtheilen, bemerke man dass

$$\cos^4 x = \frac{3 + 4 \cos 2x + \cos 4x}{8} \equiv 1 \pmod{8},$$

folglich

$$\frac{\sin x}{\cos x} \equiv \sin x \cos^3 x = \frac{2 \sin 2x + \sin 4x}{8} \equiv x - 2 \frac{x^3}{3} \pmod{8}$$

ist. Der Tangentencoefficient  $\alpha_n$  ist also durch  $8$  theilbar, sobald  $n > 2$ .<sup>1</sup>

Ähnliche Sätze gelten für die Entwicklungscoefficienten  $\gamma_n$  und  $\vartheta_n$  der Functionen  $\frac{\sin x}{\cos 2x}$  und  $\frac{\cos x}{\cos 2x}$ . Beispielsweise folgt aus der Congruenz

<sup>1</sup> Diese Thatsache geht übrigens auch aus der Gleichung  $\alpha_n = \frac{2^{2n}(2^{2n}-1)}{2n} B_n$

hervor, nach welcher  $2^{2n-\lambda-2}$  die höchste in  $\alpha_n$  aufgehende Potenz von  $2$  ist, wenn  $2^\lambda$  die höchste in  $n$  aufgehende Potenz von  $2$  bezeichnet.

Wegen der auf die Tangentencoefficienten und Euler'schen Zahlen bezüglichen Congruenzen vergleiche man die Vorlesungen über die Bernoullischen Zahlen von L. SAAL-SCHÜTZ (Berlin 1893), in welchen auch die Litteratur angegeben ist.

$$\cos 2x \equiv 1 - 2x^2 \pmod{8},$$

$$\frac{1}{\cos 2x} \equiv \frac{1}{1 - 2x^2} \equiv 1 + 2x^2 \pmod{8}$$

und hieraus weiter

$$\left. \begin{aligned} \frac{\sin x}{\cos 2x} &\equiv \sin x(1 + 2x^2) \\ \frac{\cos x}{\cos 2x} &\equiv \cos x(1 + 2x^2) \end{aligned} \right\} \pmod{8}.$$

Die letzten Congruenzen besagen, dass  $\gamma_n \equiv 1$  oder  $3 \pmod{8}$  und  $\delta_n \equiv 3$  oder  $1 \pmod{8}$  ist, je nachdem der Index  $n$  ungerade oder gerade ist.

#### 4.

Wenn  $p$  eine Primzahl ist und zur Abkürzung  $\frac{p-1}{2} = p'$  gesetzt wird, so hat man die Congruenz

$$\left(\frac{s}{p}\right) \equiv s^{p'} \pmod{p}.$$

Daher wird für den Fall, dass  $p \equiv 3 \pmod{4}$  ist,

$$h(p) \equiv 1^{p'} + 2^{p'} + 3^{p'} + \dots + p'^{p'} \pmod{p}.$$

Die auf der rechten Seite dieser Congruenz befindliche Zahl ist nichts anderes wie der Coefficient von  $(-1)^{\frac{p'-1}{2}} \cdot \frac{x^{p'}}{p'}$  in der Entwicklung der Function

$$\varphi(x) = \sin x + \sin 2x + \dots + \sin p'x = \frac{\cos \frac{1}{2}x - \cos \frac{p'}{2}x}{2 \sin \frac{1}{2}x}.$$

Nun ist nach dem Modul  $p$

$$\cos \frac{1}{2}x - \cos \frac{p'}{2}x \equiv \cos \frac{1}{2}x - 1,$$

und nach dem Satze 8 in N° 2 ist die Congruenz

$$\varphi(x) \equiv \frac{\cos \frac{1}{2}x - 1}{2 \sin \frac{1}{2}x} \equiv -\frac{1}{2} \frac{\sin \frac{x}{4}}{\cos \frac{x}{4}} \pmod{p}$$

bis zu den Gliedern  $(p-1)^{\text{ter}}$  Ordnung gültig. Also ist  $h(p)$  nach dem Modul  $p$  dem Coefficienten von  $(-1)^{\frac{p'-1}{2}} \cdot \frac{x^{p'}}{\underline{p}'}$  in der Entwicklung von  $-\frac{1}{2} \operatorname{tg} \frac{x}{4}$  congruent. Da dieser Coefficient sich modulo  $p$  nicht ändert, wenn  $x$  durch  $4x$  ersetzt wird, weil er dadurch den Factor  $4^{p'} = 2^{p'-1} \equiv 1 \pmod{p}$  erhält, so ist auch  $h(p)$  dem mit  $(-1)^{\frac{p'-1}{2}+1} = (-1)^{\frac{p+1}{4}}$  multiplicirten Coefficienten von  $\frac{x^{p'}}{\underline{p}'}$  in der Entwicklung von  $\frac{1}{2} \operatorname{tg} x$  congruent, welches die Behauptung des Satzes 1 in N° 1 ist.

Ist  $p$  eine Primzahl von der Form  $4n+1$ , so wird

$$h(p) \equiv 2 \left( 1^{p'} + 2^{p'} + \dots + \left(\frac{p'}{2}\right)^{p'} \right) \pmod{p}.$$

Die rechte Seite dieser Congruenz ist der Coefficient von  $(-1)^{\frac{p'}{2}} \cdot \frac{x^{p'}}{\underline{p}'}$  in der Entwicklung von

$$\varphi(x) = 2 \left( \cos x + \cos 2x + \dots + \cos \frac{p'}{2}x \right) = -1 + \frac{\sin \frac{p'+1}{4}x}{\sin \frac{1}{2}x}.$$

Bis zu den Gliedern von der Ordnung  $p-1$  ist aber

$$\varphi(x) \equiv -1 + \frac{\sin \frac{1}{4}x}{\sin \frac{1}{2}x} \equiv -1 + \frac{1}{2 \cos \frac{1}{4}x} \pmod{p}.$$

Diese Congruenz enthält den Satz 2. von N° 1, wenn man die Bemerkung hinzunimmt, dass der Coefficient von  $\frac{x^{p'}}{\underline{p}'}$  sich modulo  $p$  nicht ändert, falls  $x$  durch  $4x$  ersetzt wird.

Ist  $p$  eine Primzahl von der Form  $4n + 3$ , so hat man

$$h(2p) = 2 \sum_{\omega}^{3\omega} \left(\frac{s}{p}\right) = 2 \sum_0^{3\omega} \left(\frac{s}{p}\right) - 2 \sum_0^{\omega} \left(\frac{s}{p}\right), \quad \left(\omega = \frac{1}{8}p\right).$$

Die Summation in den beiden letzten Summen ist zu erstrecken auf die Zahlen

$$s = 1, 2, \dots, k \quad \text{bezüglich} \quad s = 1, 2, \dots, h$$

wo

$$k = \frac{3p-1}{8}, \quad h = \frac{p-3}{8} \quad \text{oder} \quad k = \frac{3p-5}{8}, \quad h = \frac{p-7}{8}$$

ist, je nachdem  $p \equiv 3$  oder  $\equiv 7 \pmod{8}$  ist.

Die Classenzahl  $h(2p)$  ist nun  $\pmod{p}$  congruent dem Coefficienten von  $(-1)^{\frac{p-1}{2}} \frac{x^{p'}}{\sqrt{p}}$  in der Entwicklung von

$$\varphi(x) = 2 \sum_1^k \sin(sx) - 2 \sum_1^h \sin(sx) = \frac{\cos\left(h + \frac{1}{2}\right)x - \cos\left(k + \frac{1}{2}\right)x}{\sin \frac{1}{2}x}.$$

Bis zu den Gliedern von der Ordnung  $p - 1$  ist aber

$$\varphi(x) \equiv \frac{\cos \frac{1}{8}x - \cos \frac{3}{8}x}{\sin \frac{1}{2}x} \quad \text{oder} \quad \frac{\cos \frac{3}{8}x - \cos \frac{1}{8}x}{\sin \frac{1}{2}x} \pmod{p}$$

je nachdem  $p \equiv 3$  oder  $\equiv 7 \pmod{8}$ . Ferner ist

$$\frac{\cos \frac{3}{8}x - \cos \frac{1}{8}x}{\sin \frac{1}{2}x} = - \frac{\sin \frac{1}{8}x}{\cos \frac{1}{4}x}.$$

Ersetzt man nun  $x$  durch  $8x$ , so wird sich der Coefficient von  $\frac{x^{p'}}{\sqrt{p}}$  nicht ändern  $\pmod{p}$ , wenn  $p \equiv 7 \pmod{8}$  ist, dagegen den Factor  $-1 \pmod{p}$  erhalten, wenn  $p \equiv 3 \pmod{8}$  ist, weil im ersteren Falle 2 quadratischer Rest, im letzteren Falle quadratischer Nichtrest von  $p$  ist. Hiernach leuchtet ein, dass in beiden Fällen  $h(2p)$  nach dem Modul  $p$  congruent

dem mit  $(-1)^{\frac{p-1}{2}+1} = (-1)^{\frac{p+1}{4}}$  multiplicirten Coefficienten von  $\frac{x^p}{p}$  in der Entwicklung von  $\frac{\sin x}{\cos 2x}$  ist.

Ist endlich  $p$  eine Primzahl von der Form  $4n + 1$ , so hat man

$$h(2p) = 2 \left\{ \sum_0^{\omega} \binom{s}{p} + \sum_0^{3\omega} \binom{s}{p} - \sum_0^{4\omega} \binom{s}{p} \right\}, \quad \left( \omega = \frac{1}{8}p \right)$$

oder, da  $\sum_0^{4\omega} \binom{s}{p}$  verschwindet;

$$h(2p) = 2 \left\{ \sum_0^{\omega} \binom{s}{p} + \sum_0^{3\omega} \binom{s}{p} \right\}.$$

Die Classenzahl  $h(2p)$  ist daher nach dem Modul  $p$  congruent dem Coefficienten von  $(-1)^{\frac{p}{2}} \cdot \frac{x^p}{p}$  in der Entwicklung von

$$\varphi(x) = 2 \sum_{s=1}^k \cos sx + 2 \sum_{s=1}^h \cos sx = -1 + \frac{\sin \left( k + \frac{1}{2} \right) x + \sin \left( h + \frac{1}{2} \right) x}{\sin \frac{1}{2} x},$$

wobei

$$k = \frac{p-1}{8}, \quad h = \frac{3p-3}{8} \quad \text{oder} \quad k = \frac{p-5}{8}, \quad h = \frac{3p-7}{8}$$

zu nehmen ist, je nachdem  $p \equiv 1$  oder  $\equiv 5 \pmod{8}$  ist.

Bis zu den Gliedern  $(p-1)^{\text{ter}}$  Ordnung ist nun

$$\varphi(x) \equiv -1 + \frac{\cos \frac{1}{8} x}{\cos \frac{1}{4} x} \quad \text{oder} \quad \equiv -1 - \frac{\cos \frac{1}{8} x}{\cos \frac{1}{4} x} \pmod{p},$$

je nachdem  $p \equiv 1$  oder  $\equiv 5 \pmod{8}$  ist, und hieraus geht durch eine ähnliche Überlegung, wie oben (indem man  $x$  durch  $8x$  ersetzt), die Richtigkeit des Satzes 4. in N° 1 hervor.



5.

Die Sätze dieser Nummer beziehen sich auf die Classenzahl  $h(P)$ , wo  $P$  mehrere Primfactoren enthält und  $\equiv 3 \pmod{4}$  ist. Ich zerlege  $P$  in zwei Factoren  $p$  und  $q$ , setze also

$$P = pq.$$

Über diese Factoren mache ich vorläufig nur die Voraussetzung, dass sie beide grösser als 1 sind.

Nun ist

$$h(P) = \sum \binom{s}{pq} = \sum \binom{s}{p} \binom{s}{q},$$

wo der Summationsbuchstabe  $s$  alle zwischen 0 und  $\frac{1}{2}pq$  liegenden ganzen Zahlen durchlaufen muss. Indem ich diejenigen Glieder der Summe zusammenfasse, die modulo  $q$  congruenten Werthen von  $s$  entsprechen, erhalte ich

$$h(P) = \binom{1}{q} \sum_k \binom{qk+1}{p} + \binom{2}{q} \sum_k \binom{qk+2}{p} + \dots \\ + \binom{q-1}{q} \sum_k \binom{qk+q-1}{p},$$

oder kürzer:

$$h(P) = \sum_i^q \binom{i}{q} \sum_k \binom{qk+i}{p}.$$

Die innere Summation erstreckt sich dabei über diejenigen Werthe von  $k$ , für welche  $qk+i$  zwischen 0 und  $\frac{pq}{2}$ , also  $k$  zwischen  $-\frac{i}{q}$  und  $\frac{p}{2} - \frac{i}{q} = \frac{p-1}{2} + \left(\frac{1}{2} - \frac{i}{q}\right)$  liegt. Es nimmt also  $k$  die Werthe 0, 1, 2, ...,  $\frac{p-1}{2}$  an, wenn  $i < \frac{q}{2}$ , dagegen die Werthe 0, 1, 2, ...,  $\frac{p-1}{2} - 1$ , wenn  $i > \frac{q}{2}$ .

Daher ist

$$h(P) = \sum_{i=0}^{\frac{q}{2}} \binom{i}{q} \sum_0^{\frac{p}{2}} \binom{qk+i}{p} + \sum_{i=\frac{q}{2}}^q \binom{i}{q} \sum_0^{\frac{p}{2}-1} \binom{qk+i}{p}.$$

In der zweiten Summe ersetze ich  $i$  durch  $q - i$  und erhalte unter Anwendung der Gleichung  $\left(\frac{-1}{pq}\right) = \left(\frac{-1}{p}\right)\left(\frac{-1}{q}\right) = -1$ ,

$$h(P) = \sum_0^{\frac{q}{2}} \left(\frac{i}{q}\right) \sum_0^{\frac{p}{2}} \left(\frac{qk+i}{p}\right) - \sum_0^{\frac{q}{2}} \left(\frac{i}{q}\right) \sum_1^{\frac{p}{2}} \left(\frac{i-qk}{p}\right).$$

Da nun die Zahl  $i + qk$  ein vollständiges Restsystem (mod.  $p$ ) durchläuft, wenn  $k$  alle ganze Zahlen zwischen  $-\frac{p}{2}$  und  $+\frac{p}{2}$  annimmt, so ist

$$\sum_0^{\frac{p}{2}} \left(\frac{qk+i}{p}\right) + \sum_1^{\frac{p}{2}} \left(\frac{i-qk}{p}\right) = 0, \text{ und folglich}$$

$$(I) \quad h(pq) = 2 \sum_0^{\frac{q}{2}} \left(\frac{i}{q}\right) \sum_0^{\frac{p}{2}} \left(\frac{i+qk}{p}\right).$$

Es sei jetzt  $p$  eine Primzahl von der Form  $4n + 3$ . Dann lehrt die vorstehende Gleichung, dass

$$h(pq) \equiv (-1)^{\frac{p-3}{4}} \left\{ 2 \sum_0^{\frac{q}{2}} \left(\frac{i}{q}\right) \sum_0^{\frac{p}{2}} \sin(i+qk)x \right\} \pmod{p}$$

ist, wo die geschwungene Klammer den Coefficienten von  $\frac{x^{\frac{p-1}{2}}}{\frac{p-1}{2}}$  in der

Entwicklung der eingeklammerten Function bedeutet. Nun ist weiter für jeden Werth von  $a$  und  $b$  und jedes ganzzahlige positive  $m$ :

$$(S) \quad 2 \sum_0^m \sin(a+bk) = \frac{\cos\left(a - \frac{1}{2}b\right) - \cos\left(a + \left(m + \frac{1}{2}\right)b\right)}{\sin \frac{1}{2}b}$$

$$= 2 \frac{\sin \frac{m+1}{2}b}{\sin \frac{1}{2}b} \sin\left(a + \frac{m}{2}b\right)$$

Über die Anzahl der Classen binärer quadratischer Formen von negativer Determinante. 369  
und daher bis zu den Gliedern  $(p - 1)^{\text{ter}}$  Ordnung

$$2 \sum_0^{\frac{p}{2}} \sin(i + qk)x \equiv \frac{2 \sin \frac{1}{4} qx}{\sin \frac{1}{2} qx} \sin\left(i - \frac{1}{4} q\right)x \equiv \frac{1}{\cos \frac{1}{4} qx} \sin\left(i - \frac{1}{4} q\right)x \pmod{p}.$$

Aus dieser Congruenz ergibt sich für die Classenzahl  $h(pq)$  zunächst:

$$h(pq) \equiv (-1)^{\frac{p-3}{4}} \left\{ \frac{1}{\cos \frac{1}{4} qx} \sum_0^{\frac{q}{2}} \binom{i}{q} \sin\left(i - \frac{1}{4} q\right)x \right\} \pmod{p}.$$

Hier darf offenbar  $x$  durch  $4x$  und  $\binom{i}{q}$  durch  $\binom{4i - q}{q}$  oder auch durch  $\binom{q - 4i}{q}$  ersetzt werden. Daher ist

$$h(pq) \equiv (-1)^{\frac{p+1}{4}} \left\{ \frac{1}{\cos qx} \sum_0^{\frac{q}{4}} \binom{q - 4i}{q} \sin(q - 4i)x \right. \\ \left. - \frac{1}{\cos qx} \sum_{\frac{q}{4}}^{\frac{q}{2}} \binom{4i - q}{q} \sin(4i - q)x \right\} \pmod{p}.$$

Da in der ersten Summe  $q - 4i$  alle zwischen  $q$  und  $0$  liegende Zahlen, die  $\equiv q \equiv 1 \pmod{4}$  sind, durchläuft, in der zweiten Summe  $4i - q$  alle zwischen  $0$  und  $q$  liegende Zahlen, die  $\equiv -q \equiv 3 \pmod{4}$  sind, so ist in der vorstehenden Congruenz der Satz enthalten:

I. Es sei  $q \equiv 1 \pmod{4}$  eine durch kein Quadrat ausser  $1$  theilbare positive Zahl grösser als  $1$ .

Ferner sei

$$\varphi(x) = \frac{1}{\cos qx} \left[ \binom{1}{q} \sin x - \binom{3}{q} \sin 3x + \binom{5}{q} \sin 5x - + \dots \right. \\ \left. - \binom{q-2}{q} \sin(q-2)x \right]$$

und die Entwicklung dieser Function nach Potenzen von  $x$  laute

$$\varphi(x) = c_1 x + c_2 \frac{x^3}{3} + c_3 \frac{x^5}{5} + \dots + c_n \frac{x^{2n-1}}{2n-1} + \dots$$

Bezeichnet dann  $p \equiv 3 \pmod{4}$  eine in  $q$  nicht aufgehende Primzahl, so ist

$$h(pq) \equiv (-1)^{\frac{p+1}{4}} c_{\frac{p+1}{4}} \pmod{p}.$$

Beispielsweise werden also die Reste der Classenzahlen  $h(5p)$  (modulo  $p$ ) durch die Entwicklungskoeffizienten der Function  $\frac{\sin x + \sin 3x}{\cos 5x}$  bestimmt.

Ist zweitens  $p$  eine Primzahl von der Form  $4n + 1$ , so hat man nach (1)

$$h(pq) \equiv (-1)^{\frac{p-1}{4}} \left\{ 2 \sum_0^{\frac{q}{2}} \binom{i}{q} \sum_0^{\frac{1}{2}p} \cos(i + qk)x \right\} \pmod{p}.$$

Mit Benutzung der bekannten Gleichung

$$\begin{aligned} \text{(C)} \quad 2 \sum_0^m \cos(a + bk) &= \frac{\sin\left(a + \left(m + \frac{1}{2}\right)b\right) - \sin\left(a - \frac{1}{2}b\right)}{\sin \frac{1}{2}b} \\ &= 2 \frac{\sin \frac{m+1}{2}b}{\sin \frac{1}{2}b} \cos\left(a + \frac{m}{2}b\right) \end{aligned}$$

findet man nun, dass bis zu den Gliedern der Ordnung  $p - 1$

$$2 \sum_0^{\frac{1}{2}p} \cos(i + qk)x \equiv \frac{\cos\left(i - \frac{1}{4}q\right)x}{\cos \frac{1}{4}qx}$$

ist. Hieraus schliesst man weiter

$$h(pq) \equiv (-1)^{\frac{p-1}{4}} \left\{ \frac{1}{\cos qx} \sum_0^{\frac{q}{2}} \binom{4i}{q} \cos(4i - q)x \right\} \pmod{p},$$

und da

$$\sum_0^{\frac{1}{2}q} \binom{4i}{q} \cos(4i - q)x = - \sum_0^{\frac{1}{4}q} \binom{q - 4i}{q} \cos(q - 4i)x$$

$$+ \sum_{\frac{1}{4}q}^{\frac{1}{2}q} \binom{4i - q}{q} \cos(4i - q)x$$

ist, so enthält die vorstehende Congruenz den Satz:

II. Es sei  $q \equiv 3 \pmod{4}$  eine durch kein Quadrat theilbare positive Zahl grösser als 1.

Ferner sei

$$\varphi(x) = \frac{1}{\cos qx} \left[ \binom{1}{q} \cos x - \binom{3}{q} \cos 3x + \binom{5}{q} \cos 5x - + \dots \right.$$

$$\left. + \binom{q - 2}{q} \cos(q - 2)x \right]$$

und die Entwicklung dieser Function nach Potenzen von  $x$  laute

$$\varphi(x) = c_0 + c_1 \frac{x^2}{2} + c_2 \frac{x^4}{4} + \dots + c_n \frac{x^{2n}}{2n} + \dots$$

Bezeichnet dann  $p \equiv 1 \pmod{4}$  eine in  $q$  nicht aufgehende Primzahl, so ist

$$h(pq) \equiv (-1)^{\frac{p-1}{4}} c_{\frac{p-1}{4}} \pmod{p}.$$

Für den einfachsten Fall  $q = 3$  kann man diesem Satze, da  $h(3p)$  stets kleiner als  $p$  ist, die bestimmtere Fassung geben:

Ist  $p$  eine Primzahl von der Form  $4n + 1$ , ist ferner

$$\frac{\cos x}{\cos 3x} = c_0 + c_1 \frac{x^2}{2} + \dots + c_n \frac{x^{2n}}{2n} + \dots,$$

so stimmt die Classenzahl  $h(3p)$  mit dem kleinsten positiven Rest von

$$(-1)^{\frac{p-1}{4}} c_{\frac{p-1}{4}} \pmod{p} \text{ überein.}$$

## 6.

Wenn  $P \equiv 1 \pmod{4}$  ist und  $P$  in zwei Factoren  $p$  und  $q$  zerlegt wird, so findet man

$$h(pq) = 2 \sum_0^q \binom{i}{q} \sum_k \binom{i+qk}{p},$$

wo die innere Summation über alle ganzen Zahlen  $k$  zu erstrecken ist, für welche  $i+qk$  zwischen 0 und  $\frac{1}{4}pq$  liegt, also über alle ganzen Zahlen  $k$ , die zwischen  $-\frac{i}{q}$  und  $\frac{1}{4}p - \frac{i}{q}$  liegen.

Ich trenne jetzt die Fälle  $p \equiv q \equiv 1 \pmod{4}$  und  $p \equiv q \equiv 3 \pmod{4}$ .

Im ersten Falle muss  $k$  die Werthe  $0, 1, \dots, \frac{p-1}{4}$  oder  $0, 1, \dots, \frac{p-1}{4} - 1$  durchlaufen, je nachdem  $i < \frac{q}{4}$  oder  $i > \frac{q}{4}$  ist. Daher kommt

$$h(pq) = 2 \sum_0^{\frac{1}{4}q} \binom{i}{q} \sum_0^{\frac{1}{4}p} \binom{i+qk}{p} + 2 \sum_{\frac{1}{4}q}^q \binom{i}{q} \sum_0^{\frac{1}{4}p-1} \binom{i+qk}{p}.$$

Ersetzt man in denjenigen Theilen der Summe, in welchen  $i > \frac{q}{2}$  ist,  $i$  durch  $q-i$ , so erhält man nach leichten Umformungen:

$$(1) \quad h(pq) = 2 \sum_0^{\frac{1}{4}q} \binom{i}{q} \sum_{-\frac{1}{4}p}^{\frac{1}{4}p} \binom{i+qk}{p} + 2 \sum_{\frac{1}{4}q}^{\frac{1}{2}q} \binom{i}{q} \sum_{-\frac{1}{4}p}^{\frac{1}{4}p-1} \binom{i+qk}{p},$$

$(p \equiv q \equiv 1 \pmod{4}).$

Im zweiten Falle findet man in ähnlicher Weise:

$$(2) \quad h(pq) = 2 \sum_0^{\frac{1}{4}q} \binom{i}{q} \sum_{-\frac{1}{4}p}^{\frac{1}{4}p} \binom{i+qk}{p} + 2 \sum_{\frac{1}{4}q}^{\frac{1}{2}q} \binom{i}{q} \sum_{-\frac{1}{4}p-1}^{\frac{1}{4}p} \binom{i+qk}{p},$$

$(p \equiv q \equiv 3 \pmod{4}).$

Unter der Voraussetzung, dass  $p$  eine Primzahl ist, findet im ersten Falle die Congruenz

$$(1') \quad h(pq) \equiv (-1)^{\frac{p-1}{4}} \left\{ 2 \sum_0^{\frac{1}{4}q} \left(\frac{i}{q}\right) \sum_{-\frac{1}{4}p}^{\frac{1}{4}p} \cos(i + qk)x \right. \\ \left. + 2 \sum_{\frac{1}{4}q}^{\frac{1}{2}q} \left(\frac{i}{q}\right) \sum_{-\frac{1}{4}p}^{\frac{1}{4}p-1} \cos(i + qk)x \right\} \pmod{p}$$

im zweiten Falle die Congruenz

$$(2') \quad h(pq) \equiv (-1)^{\frac{p-3}{4}} \left\{ 2 \sum_0^{\frac{1}{4}q} \left(\frac{i}{q}\right) \sum_{-\frac{1}{4}p}^{\frac{1}{4}p} \sin(i + qk)x \right. \\ \left. + 2 \sum_{\frac{1}{4}q}^{\frac{1}{2}q} \left(\frac{i}{q}\right) \sum_{-\frac{1}{4}p-1}^{\frac{1}{4}p} \sin(i + qk)x \right\} \pmod{p}$$

statt. Dabei bedeutet die geschwungene Klammer, wie oben, den Coefficienten von  $\frac{x^{\frac{p-1}{2}}}{\frac{p-1}{2}}$  in der Entwicklung der eingeklammerten Function.

Diese Congruenzen lassen sich mit Hülfe der Formeln (S) und (C) der vorigen Nummer und der Sätze von N° 2 in die folgenden einfacheren Congruenzen überführen:

$$h(pq) \equiv (-1)^{\frac{p-1}{4}} \left\{ \frac{1}{\cos qx} \sum_0^{\frac{1}{4}q} \left(\frac{4i}{q}\right) \cos 4ix \right. \\ \left. - \frac{1}{\cos qx} \sum_{\frac{1}{4}q}^{\frac{1}{2}q} \left(\frac{2q-4i}{q}\right) \cos(2q-4i)x \right\} \pmod{p}$$

bezüglich

$$h(pq) \equiv (-1)^{\frac{p-3}{4}} \left\{ -\frac{1}{\cos qx} \sum_0^{\frac{1}{4}q} \binom{4i}{q} \sin 4ix \right. \\ \left. + \frac{1}{\cos qx} \sum_{\frac{1}{4}q}^{\frac{1}{2}q} \binom{2q-4i}{q} \sin(2q-4i)x \right\} \pmod{p}.$$

Diese Congruenzen enthalten nun folgende Sätze, die sich den Sätzen I. und II. der vorigen Nummer an die Seite stellen:

III. *Es sei  $q \equiv 1 \pmod{4}$  eine durch kein Quadrat ausser 1 theilbare positive Zahl grösser als 1. Ferner sei*

$$\varphi(x) = \frac{1}{\cos qx} \left[ -\binom{2}{q} \cos 2x + \binom{4}{q} \cos 4x - \binom{6}{q} \cos 6x + \dots \right. \\ \left. + \binom{q-1}{q} \cos(q-1)x \right]$$

und die Entwicklung dieser Function nach Potenzen von  $x$  laute

$$\varphi(x) = c_0 + c_1 \frac{x^2}{2} + \dots + c_n \frac{x^{2n}}{2n} + \dots$$

Bezeichnet dann  $p \equiv 1 \pmod{4}$  eine in  $q$  nicht aufgehende Primzahl, so ist

$$h(pq) \equiv (-1)^{\frac{p-1}{4}} c_{\frac{p-1}{4}} \pmod{p}.$$

IV. *Es sei  $q \equiv 3 \pmod{4}$  eine durch kein Quadrat ausser 1 theilbare positive Zahl grösser als 1. Ferner sei*

$$\varphi(x) = \frac{1}{\cos qx} \left[ \binom{2}{q} \sin 2x - \binom{4}{q} \sin 4x + \binom{6}{q} \sin 6x - \dots \right. \\ \left. + \binom{q-1}{q} \sin(q-1)x \right]$$

und die Entwicklung dieser Function nach Potenzen von  $x$  laute:

$$\varphi(x) = c_1 x + c_2 \frac{x^3}{3} + \dots + c_n \frac{x^{2n-1}}{2n-1} + \dots$$



Bezeichnet dann  $p \equiv 3 \pmod{4}$  eine in  $q$  nicht aufgehende Primzahl, so ist

$$h(pq) \equiv (-1)^{\frac{p-3}{4}} c_{\frac{p+1}{4}} \pmod{p}.$$

In dem besonderen Falle  $q = 3$  hat man den bestimmteren Satz, dass — unter  $p$  eine von 3 verschiedene Primzahl der Form  $4n + 3$  verstanden — die Classenzahl  $h(3p)$  gleich ist dem kleinsten positiven Reste von  $(-1)^{\frac{p+1}{4}} c_{\frac{p+1}{4}} \pmod{p}$ , wenn  $c_n$  den Coefficienten von  $\frac{x^{2n-1}}{2n-1}$  in der Potenzentwicklung von  $\frac{\sin 2x}{\cos 3x}$  bezeichnet.

## 7.

Analoge Sätze, wie sie für die Classenzahl  $h(pq)$  in den letzten beiden Nummern aufgestellt sind, bestehen für die Classenzahl  $h(2pq)$ . Ich gebe diese Sätze hier an, gehe jedoch auf ihre Beweise nicht ein, da die letzteren ziemlich umständlich sind, ohne gegenüber den Beweisen der Sätze in N<sup>o</sup> 5 und 6 neue Momente darzubieten. Die Sätze lauten folgendermassen:

V. Es sei  $q \equiv 1 \pmod{4}$  eine durch kein Quadrat ausser 1 theilbare positive Zahl grösser als 1. Ferner sei

$$\begin{aligned} \varphi_1(x) = \frac{1}{\cos 2qx} & \left[ \left(\frac{1}{q}\right) \cos x - \left(\frac{3}{q}\right) \cos 3x - \left(\frac{5}{q}\right) \cos 5x + \left(\frac{7}{q}\right) \cos 7x + \dots \right. \\ & \left. + \left(\frac{2q-1}{q}\right) \cos(2q-1)x \right] \end{aligned}$$

und

$$\begin{aligned} \varphi_2(x) = \frac{1}{\cos 2qx} & \left[ \left(\frac{1}{q}\right) \sin x + \left(\frac{3}{q}\right) \sin 3x - \left(\frac{5}{q}\right) \sin 5x - \left(\frac{7}{q}\right) \sin 7x + \dots \right. \\ & \left. + \left(\frac{2q-1}{q}\right) \sin(2q-1)x \right]. \end{aligned}$$

Der Coefficient von  $\frac{x^{2n}}{\lfloor 2n \rfloor}$  in der Potenzentwicklung von  $\varphi_1(x)$  werde mit  $c_n$ , der Coefficient von  $\frac{x^{2n-1}}{\lfloor 2n-1 \rfloor}$  in der Entwicklung von  $\varphi_2(x)$  mit  $d_n$  bezeichnet.

Ist dann  $p$  eine nicht in  $q$  aufgehende Primzahl, so besteht die Congruenz

$$h(2pq) \equiv (-1)^{\frac{p-1}{4}} c_{\frac{p-1}{4}} \pmod{p}$$

oder die Congruenz

$$h(2pq) \equiv (-1)^{\frac{p+1}{4}} d_{\frac{p+1}{4}} \pmod{p},$$

je nachdem  $p \equiv 1$  oder  $\equiv 3 \pmod{4}$  ist.

VI. Es sei  $q \equiv 3 \pmod{4}$  eine durch kein Quadrat ausser 1 theilbare positive Zahl grösser als 1. Ferner sei

$$\begin{aligned} \varphi_1(x) = \frac{1}{\cos 2qx} & \left[ \left(\frac{1}{q}\right) \cos x + \left(\frac{3}{q}\right) \cos 3x - \left(\frac{5}{q}\right) \cos 5x - \left(\frac{7}{q}\right) \cos 7x + \dots \right. \\ & \left. - \left(\frac{2q-1}{q}\right) \cos (2q-1)x \right], \end{aligned}$$

$$\begin{aligned} \varphi_2(x) = \frac{1}{\cos 2qx} & \left[ \left(\frac{1}{q}\right) \sin x - \left(\frac{3}{q}\right) \sin 3x - \left(\frac{5}{q}\right) \sin 5x + \left(\frac{7}{q}\right) \sin 7x + \dots \right. \\ & \left. - \left(\frac{2q-1}{q}\right) \sin (2q-1)x \right] \end{aligned}$$

und die Coefficienten von  $\frac{x^{2n}}{\lfloor 2n \rfloor}$  bez.  $\frac{x^{2n-1}}{\lfloor 2n-1 \rfloor}$  in den Potenzentwicklungen von  $\varphi_1(x)$  bez.  $\varphi_2(x)$  mögen mit  $c_n$  bez.  $d_n$  bezeichnet werden.

Ist dann  $p$  eine nicht in  $q$  aufgehende Primzahl, so besteht die Congruenz

$$h(2pq) \equiv (-1)^{\frac{p-1}{4}} c_{\frac{p-1}{4}} \pmod{p}$$

oder die Congruenz

$$h(2pq) \equiv (-1)^{\frac{p+1}{4}} d_{\frac{p+1}{4}} \pmod{p},$$

je nachdem  $p \equiv 1$  oder  $\equiv 3 \pmod{4}$  ist.

In dem besondern Falle  $q = 3$  wird  $\varphi_1(x) = \frac{\cos x + \cos 5x}{\cos 6x}$  und  $\varphi_2(x) = \frac{\sin x + \sin 5x}{\cos 6x}$  und durch die Congruenzen des Satzes VI sind die Classenzahlen  $h(6p)$  vollkommen bestimmt, da sie die Zahl  $p$  nicht überschreiten können.

## 8.

Die vorstehend entwickelten Sätze gestatten eine Ergänzung dadurch, dass man das Verhalten der Classenzahlen in Bezug auf die Potenzen von 2 als Moduln in Rücksicht zieht. Die Theorie der Genera lehrt in dieser Hinsicht Folgendes.<sup>1</sup> Wenn  $\lambda$  die Zahl der Primfactoren bezeichnet, aus denen sich  $P$  zusammensetzt, so ist  $h(P)$  durch  $2^{\lambda-1}$  oder  $2^\lambda$  theilbar, je nachdem  $P \equiv 3$  oder  $\equiv 1 \pmod{4}$  ist, während  $h(2P)$  stets durch  $2^\lambda$  theilbar ist. Bedeutet nämlich  $h_g(P)$  die Anzahl der Classen eigentlich primitiver positiver Formen der Determinante  $-P$ , die in dem einzelnen Genus enthalten sind, so ist bekanntlich

$$h_g(P) = \frac{1}{2^{\lambda-1}} h(P), \quad \text{wenn } P \equiv 3 \pmod{4},$$

$$h_g(P) = \frac{1}{2^\lambda} h(P), \quad \text{wenn } P \equiv 1 \pmod{4},$$

$$h_g(2P) = \frac{1}{2^\lambda} h(2P).$$

Man kann aber hierüber hinaus in den Fällen  $\lambda = 1$  und  $\lambda = 2$  in einfacher Weise entscheiden, ob  $h_g(P)$  bez.  $h_g(2P)$  congruent 0 oder 1 (mod. 2) ist, ob also das einzelne Genus eine gerade oder ungerade Anzahl von Classen umfasst.

Wenn zunächst  $\lambda = 1$ , also  $P = p$  eine Primzahl ist, so bestehen die folgenden Congruenzen:

---

<sup>1</sup> DIRICHLET, *Vorlesungen über Zahlentheorie*. (Supplement IV.)

*Acta mathematica*. 19. Imprimé le 7 août 1895.

$$h_g(p) = h(p) \equiv 1 \pmod{2}, \quad \text{wenn } p \equiv 3 \pmod{4},^1$$

$$h_g(p) = \frac{1}{2}h(p) \equiv \frac{p-1}{2} \pmod{2}, \quad \text{wenn } p \equiv 1 \pmod{4},$$

$$h_g(2p) = \frac{1}{2}h(2p) \equiv \frac{p^2-1}{8} \pmod{2}.$$

Wenn  $\lambda = 2$ , also  $P = pq$  ist, wo  $p$  und  $q$  zwei von einander verschiedene ungerade Primzahlen sind, so hängt der Rest von  $h_g(P)$  resp.  $h_g(2P) \pmod{2}$  einerseits von dem Werthe des Legendre'schen Zeichens  $\left(\frac{p}{q}\right)$ , andererseits von den Resten der Zahlen  $p$  und  $q \pmod{8}$  ab. In jedem einzelnen Falle lehren die folgenden beiden Tabellen, ob  $h_g(pq)$  bez.  $h_g(2pq)$  eine gerade oder ungerade Zahl ist. In den Tabellen bedeutet  $\varepsilon$  die Abkürzung für  $\frac{1}{2}\left(1 - \left(\frac{p}{q}\right)\right)$ , es ist also

$$\varepsilon = 0 \quad \text{oder} \quad \varepsilon = 1,$$

je nachdem  $p$  quadratischer Rest oder quadratischer Nichtrest von  $q$  ist.

**Tabelle für die Reste von  $h_g(pq)$  nach dem Modul 2.**

	$q \equiv 1$	$q \equiv 3$	$q \equiv 5$	$q \equiv 7$
$p \equiv 1$	0	$\varepsilon$	$\varepsilon$	$\varepsilon$
$p \equiv 3$	$\varepsilon$	1	$\varepsilon$	$\varepsilon$
$p \equiv 5$	$\varepsilon$	$\varepsilon$	0	$\varepsilon$
$p \equiv 7$	$\varepsilon$	$1 - \varepsilon$	$\varepsilon$	0

Die Einrichtung der Tabelle ist diese: In dem einzelnen Felde der Tabelle findet sich der Rest von  $h_g(pq) \pmod{2}$ , so oft  $p$  und  $q$  nach

<sup>1</sup> Nach dem Modul 4 ist  $h(p) \equiv \frac{p-1}{2}$  od.  $\frac{p+3}{2}$ , je nachdem  $\left|\frac{p-1}{2}\right| \equiv +1$  oder  $-1 \pmod{4}$  ist. Vgl. JACOBI, *Observatio arithmetica de numero classium divisorum* etc., Crelles Journal, Bd. 9 oder Werke, Bd. 6 pag. 240.

dem Modul 8 die Congruenzen befriedigen, welche die in dem Felde sich kreuzenden Horizontal- bez. Verticalreihen characterisiren. Beispielsweise ist  $h_g(pq) \equiv \varepsilon \pmod{2}$  falls  $p \equiv 3$  und  $q \equiv 5 \pmod{8}$  ist. Die Anzahl der im einzelnen Genus enthaltenen Classen ist dann also gerade oder ungerade, je nachdem  $p$  Rest oder Nichtrest von  $q$  ist.

In der gleichen Weise ist die folgende Tabelle eingerichtet:

Tabelle für die Reste von  $h_g(2pq) = \frac{1}{4}h(2pq)$  nach dem Modul 2.

	$q \equiv 1$	$q \equiv 3$	$q \equiv 5$	$q \equiv 7$
$p \equiv 1$	0	$\varepsilon$	$\varepsilon$	0
$p \equiv 3$	$\varepsilon$	0	1	$\varepsilon$
$p \equiv 5$	$\varepsilon$	1	1	$\varepsilon$
$p \equiv 7$	0	$1 - \varepsilon$	$\varepsilon$	0

Was die Beweise dieser auf die Zahlen  $h_g$  bezüglichen Sätze angeht, so möge es genügen, einen besonderen Fall zu betrachten, bei welchem das Princip der Beweise klar hervortritt.

Es sei  $P = pq \equiv 1 \pmod{4}$  das Produkt zweier Primzahlen; dann ist

$$h_g = h_g(2pq) = \frac{1}{4}h(2pq) = \frac{1}{2} \left[ \sum_0^{\frac{1}{8}pq} \left( \frac{s}{pq} \right) + \sum_0^{\frac{3}{8}pq} \left( \frac{s}{pq} \right) \right].$$

Wenn nun die Anzahl der Jacobi'schen Zeichen  $\left( \frac{s}{pq} \right)$ , die den Werth  $+1$  bezüglich  $-1$  besitzen, in der ersten Summe mit  $A$  bezüglich  $B$ , in der zweiten Summe mit  $A'$  bezüglich  $B'$  bezeichnet wird, so ist

$$h_g = \frac{1}{2}(A - B + A' - B') = \frac{1}{2}(A + B) + \frac{1}{2}(A' + B') - (B + B').$$

Die Zahlen  $A + B$  und  $A' + B'$  geben an, wie viele Zahlen  $s$  zwischen



wo  $k = \left[ \frac{q}{8} \right]$  und  $a_2 = \left[ \frac{pq}{8} \right] - p \left[ \frac{q}{8} \right]$  ist. Nach dem Wilson'schen Lehrsatze wird daher

$$\prod \binom{s_1}{p} \prod_{r=1}^{a_1} \binom{rq}{p} = \left( \frac{-1}{p} \right)^{\left[ \frac{q}{8} \right]} \left( \frac{a_2}{p} \right),$$

oder

$$\prod \binom{s_1}{p} = \left( \frac{-1}{p} \right)^{\left[ \frac{q}{8} \right]} \left( \frac{q}{p} \right)^{\left[ \frac{p}{8} \right]} \left( \frac{a_1}{p} \right) \left( \frac{a_2}{p} \right).$$

In analoger Weise lässt sich  $\prod \binom{s_2}{p}$  umformen, und so findet man schliesslich

$$\Pi_p = \left( \frac{-1}{p} \right)^{\left[ \frac{q}{8} \right] + \left[ \frac{3q}{8} \right]} \left( \frac{q}{p} \right)^{\left[ \frac{p}{8} \right] + \left[ \frac{3p}{8} \right]} \left( \frac{a_1 | a_2 | a_3 | a_4}{p} \right)$$

wo  $a_1, a_2, a_3, a_4$  die folgende Bedeutung haben

$$a_1 = \left[ \frac{p}{8} \right], \quad a_2 = \left[ \frac{pq}{8} \right] - p \left[ \frac{q}{8} \right], \quad a_3 = \left[ \frac{3p}{8} \right], \quad a_4 = \left[ \frac{3pq}{8} \right] - p \left[ \frac{3q}{8} \right].$$

Wenn nun  $q \equiv 1$  oder  $3 \pmod{8}$ , so ergibt sich leicht, dass  $a_2 = a_1$ ,  $a_4 = a_3$  oder  $a_2 = a_3$ ,  $a_4 = a_1$  und daher  $\left( \frac{a_1 | a_2 | a_3 | a_4}{p} \right) = +1$  ist.

Dasselbe Legendre'sche Zeichen hat dagegen den Werth  $\left( \frac{-1}{p} \right)^{\left[ \frac{p}{8} \right] + \left[ \frac{3p}{8} \right]}$ , wenn  $q \equiv 5$  oder  $7 \pmod{8}$  ist. Denn in diesen Fällen ist  $a_2 = \left[ \frac{5p}{8} \right]$ ,  $a_4 = \left[ \frac{7p}{8} \right]$  oder  $a_2 = \left[ \frac{7p}{8} \right]$ ,  $a_4 = \left[ \frac{5p}{8} \right]$ .

Aus dem Wilson'schen Satze folgt aber, dass

$$\left[ \frac{p}{8} \right] \left[ \frac{7p}{8} \right] \equiv (-1)^{\left[ \frac{p}{8} \right]} \quad \text{und} \quad \left[ \frac{3p}{8} \right] \left[ \frac{5p}{8} \right] \equiv (-1)^{\left[ \frac{3p}{8} \right]} \pmod{p} \text{ ist.}$$

Zusammenfassend kann man sagen, dass

$$\Pi_p = \left( \frac{-1}{p} \right)^{\left[ \frac{q}{8} \right] + \left[ \frac{3q}{8} \right]} \left( \frac{\pm q}{p} \right)^{\left[ \frac{p}{8} \right] + \left[ \frac{3p}{8} \right]}$$

ist, wo das doppelte Vorzeichen nach der Massgabe zu bestimmen ist, dass  $\pm q \equiv 1$  oder  $3 \pmod{8}$  wird. In entsprechender Weise hat man natürlich

$$H_q = \left(\frac{-1}{q}\right)^{\left[\frac{p}{8}\right] + \left[\frac{3p}{8}\right]} \left(\frac{\pm p}{q}\right)^{\left[\frac{q}{8}\right] + \left[\frac{3q}{8}\right]},$$

wo das doppelte Vorzeichen wieder durch die Forderung  $\pm p \equiv 1$  oder  $3 \pmod{8}$  zu bestimmen ist.

Hiernach kann man für den Fall  $pq \equiv 1 \pmod{4}$  den Rest von  $h_q(2pq) \pmod{2}$  leicht feststellen, wenn die Reste von  $p$  und  $q \pmod{8}$  sowie das Vorzeichen  $\left(\frac{p}{q}\right)$  bekannt sind. Unterscheidet man je nach den Resten von  $p$  und  $q \pmod{8}$  einzelne Unterfälle, so ergeben sich die in der zweiten Tabelle auf die Fälle  $p \equiv 1, 5$ ;  $q \equiv 1, 5$  und  $p \equiv 3, 7$ ;  $q \equiv 3, 7 \pmod{8}$  bezüglichen Angaben.

## 9.

Mit Hilfe der Sätze von N° 8 lassen sich die Resultate der früheren Nummern noch ein wenig erweitern, wie ich nun noch an einigen Beispielen zeigen will.

Wenn die Zahlen  $c_1, c_2, \dots$  durch die Gleichung

$$(1) \quad \frac{\sin x + \sin 3x}{\cos 5x} = c_1 x + c_2 \frac{x^3}{3} + \dots + c_n \frac{x^{2n-1}}{2n-1} + \dots$$

erklärt werden, so findet nach Satz I in N° 5 die Congruenz statt

$$(2) \quad h(5p) \equiv (-1)^{\frac{p+1}{4}} c_{\frac{p+1}{4}} \pmod{p},$$

unter  $p$  eine Primzahl von der Form  $4n + 3$  verstanden.

Nun ist einerseits  $h(5p)$  durch 2 theilbar ( $h_q(5p) = \frac{1}{2} h(5p)$ ); andererseits ist

$$\frac{\sin x + \sin 3x}{\cos 5x} \equiv \frac{\sin x + \sin(-x)}{\cos 5x} \equiv 0 \pmod{4},$$



d. h. die Coefficienten  $c_1, c_2, \dots$  sind sämmtlich durch 4 theilbar. Daher kann die Congruenz (2) durch die folgende ersetzt werden:

$$(2') \quad h(5p) \equiv (-1)^{\frac{p+1}{4}} c_{\frac{p+1}{4}} \pmod{2p}.$$

Da nun weiter die Anzahl der Jacobi'schen Zeichen, aus denen sich  $h(5p)$  zusammensetzt,  $\left[\frac{5p}{2}\right] - \left[\frac{p}{2}\right] - \left[\frac{5}{2}\right] = 2p - 2$  beträgt, also  $h(5p) < 2p$  ist,

so folgt, dass  $h(5p)$  der kleinste positive Rest von  $(-1)^{\frac{p+1}{4}} c_{\frac{p+1}{4}} \pmod{2p}$  ist. Die Congruenz (2') kann ihrerseits durch eine Congruenz nach dem Modul  $4p$  ersetzt werden. Nach der ersten Tabelle der vorigen Nummer ist nämlich  $h(5p) \equiv 1 - \left(\frac{p}{5}\right) \pmod{4}$ , also  $h(5p) \equiv 0$  oder  $2 \pmod{4}$ , je nachdem  $p \equiv \pm 1$  oder  $\pm 2 \pmod{5}$  ist. Hiernach leuchtet ein, dass

$$(2'') \quad h(5p) \equiv (-1)^{\frac{p+1}{4}} c_{\frac{p+1}{4}} \pmod{4p}, \quad \text{für } p \equiv \pm 1 \pmod{5},$$

$$(2''') \quad h(5p) \equiv (-1)^{\frac{p+1}{4}} c_{\frac{p+1}{4}} + 2p \pmod{4p}, \quad \text{für } p \equiv \pm 2 \pmod{5}$$

ist. Ähnliche Resultate knüpfen sich an die Sätze III in N° 6 und V und VI in N° 7, so dass man beispielsweise die Classenzahlen  $h(5p)$  und  $h(10p)$  in folgender Weise durch Entwicklungscoefficienten bestimmen kann:

Es seien die Zahlen  $c, d, e, f$  durch folgende Gleichungen erklärt:

$$\frac{\sin x + \sin 3x}{\cos 5x} = \sum_1^{\infty} c_n \frac{x^{2n-1}}{2n-1},$$

$$\frac{\cos 2x + \cos 4x}{\cos 5x} = \sum_0^{\infty} d_n \frac{x^{2n}}{2n},$$

$$\frac{\sin x - \sin 3x + \sin 7x + \sin 9x}{\cos 10x} = \sum_1^{\infty} e_n \frac{x^{2n-1}}{2n-1},$$

$$\frac{\cos x + \cos 3x - \cos 7x + \cos 9x}{\cos 10x} = \sum_0^{\infty} f_n \frac{x^{2n}}{2n}.$$

Dann ist die Classenzahl  $h(5p)$  der kleinste positive nach dem Modul  $2p$  genommene Rest von  $(-1)^{\frac{p+1}{4}} c_{\frac{p+1}{4}}$  oder  $(-1)^{\frac{p-1}{4}} d_{\frac{p-1}{4}}$ , je nachdem  $p \equiv 3$  oder  $\equiv 1 \pmod{4}$  ist; die Classenzahl  $h(10p)$  stimmt überein mit dem kleinsten positiven nach dem Modul  $2p$  genommenen Rest von  $(-1)^{\frac{p+1}{4}} e_{\frac{p+1}{4}}$  oder  $(-1)^{\frac{p-1}{4}} f_{\frac{p-1}{4}}$ , je nachdem  $p \equiv 3$  oder  $\equiv 1 \pmod{4}$  ist.

Unter  $p$  ist dabei irgend eine von 5 verschiedene ungerade Primzahl zu verstehen.

---