Zur Theorie des Fermatschen Quotienten $\frac{a^{p-1}-1}{p} = q(a)$.

Von

M. Lerch in Freiburg (Schweiz).

Ist p eine ungerade Primzahl, a eine beliebige durch p nicht aufgehende ganze Zahl, so ist der Quotient

$$q(a) = \frac{a^{p-1}-1}{p} \tag{1}$$

eine ganze Zahl, welche einige verhältnismäßig einfache Kongruenz-Eigenschaften besitzt, die hier entwickelt werden sollen. Die Art der Resultate ist aus den numerierten Formeln (Gleichungen oder Kongruenzen) leicht zu übersehen.

Zunächst setzen wir die Definitionsgleichung (1) in die Gestalt

$$a^{p-1} = 1 + pq(a), \tag{1^0}$$

und bilden das Produkt der Resultate, welche den Werten $a = 1, 2, \cdots, p-1$ entsprechen. Wird der Kürze wegen

$$P = 1 \cdot 2 \cdot 3 \cdots (p-1) = (p-1)! \tag{2}$$

gesetzt, so entsteht die Gleichung

$$P^{p-1} = \prod_{a=1}^{p-1} (1 + pq(a)),$$

aus welcher sich durch Ausführung der Multiplikation rechterhand die Kongruenz

$$P^{p-1} \equiv 1 + p \sum_{a=1}^{p-1} q(a) \pmod{p^2} \tag{α}$$

erschließen läßt.

Um die linke Seite zu vereinfachen, bemerken wir, daß nach dem Wilsonschen Satze der Quotient

(3) $$\frac{P+1}{p} = N$$

eine ganze Zahl ist; die Gleichung

$$P = -1 + pN$$

ergibt aber, wenn man auf beiden Seiten auf die $(p-1)^{te}$ Potenz erhebt, nach dem binomischen Lehrsatz offenbar

$$P^{p-1} \equiv 1 - p(p-1)N \pmod{p^2},$$

oder einfacher,

$$P^{p-1} \equiv 1 + pN \pmod{p^2}.$$

Diese Kongruenz hat mit (α) den gleichen Modul und die gleiche linke Seite; dies liefert unser erstes Resultat

(4) $$\sum_{a=1}^{p-1} q(a) \equiv N \pmod{p},$$

eine Kongruenz, welche die Summe der Fermatschen mit dem Wilsonschen Quotienten in Verbindung setzt.

Zu weiteren Betrachtungen bedürfen wir der bekannten Sätze

(5) $$q(ab) \equiv q(a) + q(b) \pmod{p},$$

(6) $$q(c+pz) \equiv q(c) - \frac{z}{c} \pmod{p},$$

welche man mit betreffenden Literaturangaben in Herrn P. Bachmanns Niederer Zahlentheorie findet.

In der letzten Kongruenz (6) tritt auf der rechten Seite ein Bruch $\frac{z}{c}$ auf, unter dem man in der Regel das Produkt von z mit dem sogenannten socius c^{-1} von $c \pmod{p}$ versteht. Ich finde übrigens vorteilhafter, den Kongruenzbegriff auf Brüche auszudehnen und mit letzteren systematisch im Sinne der Kongruenz zu rechnen, was übrigens in der Zahlentheorie längst geschieht.

Ich setze nun in (5) an Stelle von b der Reihe nach die Zahlen $\nu = 1, 2, 3, \cdots, p-1$ und addiere die Ergebnisse. So entsteht zunächst

$$\sum_{\nu=1}^{p-1} q(\nu a) \equiv (p-1)\,q(a) + \sum_{\nu=1}^{p-1} q(\nu) \pmod{p}$$

oder

(β) $$\sum_{\nu=1}^{p-1} q(\nu a) \equiv -q(a) + \sum_{\nu=1}^{p-1} q(\nu) \pmod{p}.$$

In dieser Kongruenz wollen wir die linke Seite umformen, wodurch sich eine Darstellung von $q(a)$ modulo p ergeben wird.

Jeder Zahl ν der Reihe 1 bis $p-1$ entspricht eine Zahl c derselben Reihe, für welche

$$\nu a \equiv c \pmod{p}$$

oder also

$$\nu a = c + pz, \qquad (0<c<p)$$

wobei unter z eine ganze Zahl verstanden wird. Schreibt man diese Gleichung in der Gestalt

$$\frac{\nu a}{p} = \frac{c}{p} + z,$$

so läßt sich $\frac{c}{p}$ als der kleinste positive Rest und z als das größte Ganze der Größe $\frac{\nu a}{p}$, d. h.

$$z = \left[\frac{\nu a}{p}\right], \qquad c = \nu a - pz,$$

charakterisieren.

Nun wird aber nach (6) für den Modul p

$$q(\nu a) \equiv q(c+pz) \equiv q(c) - \frac{z}{c}$$

oder

$$q(\nu a) \equiv q(c) - \frac{z}{\nu a - pz} \equiv q(c) - \frac{z}{\nu a},$$

d. h. also

$$q(\nu a) \equiv q(c) - \frac{1}{\nu a}\left[\frac{\nu a}{p}\right] \pmod{p}, \tag{7}$$

wenn $0 < c < p$ und

$$\nu a \equiv c \pmod{p}.$$

Wenn bei festem a die Zahl ν die sämtlichen Werte aus der Reihe von 1 bis $p-1$ durchläuft, so nimmt c die gleichen Werte in verschiedener Reihenfolge an, d. h. es ist

$$\sum q(c) = \sum_{1}^{p-1} q(\nu),$$

und wir erhalten demnach aus (7) durch Addition

$$\sum_{\nu=1}^{p-1} q(\nu a) \equiv \sum_{1}^{p-1} q(\nu) - \sum_{\nu=1}^{p-1} \frac{1}{\nu a}\left[\frac{\nu a}{p}\right] \pmod{p}.$$

Wird dies mit (β) verglichen, so fällt in dem Resultat die Summe

$$\sum q(\nu)$$

heraus und *wir erhalten die Kongruenz*

$$q(a) \equiv \sum_{\nu=1}^{p-1} \frac{1}{\nu a}\left[\frac{\nu a}{p}\right] \pmod{p}, \tag{8}$$

welche für sämtliche durch p nicht aufgehende ganze Zahlen a besteht. Man kann sie auch so schreiben:

$$(8^*) \qquad \frac{a^p - a}{p} \equiv \sum_{\nu=1}^{p-1} \frac{1}{\nu} \left[\frac{\nu a}{p}\right] \pmod{p}.$$

Bedient man sich der hier beizubehaltenden Bezeichnung

$$\frac{p-1}{2} = m,$$

so werden für $a = 2$ auf der rechten Seite von (8*) erst die Glieder

$$\nu = m+1,\ m+2, \cdots, 2m$$

von Null verschieden sein und zwar ist

$$(9) \qquad \frac{2^p - 2}{p} \equiv \sum_{\nu=m+1}^{2m} \frac{1}{\nu} \equiv -\sum_{1}^{m} \frac{1}{\nu} \pmod{p}.$$

Die zweite Form ist nämlich eine unmittelbare Folge der ersten und des naheliegenden Umstandes, daß

$$\sum_{1}^{2m} \frac{1}{\nu} \equiv 0 \pmod{p}.$$

Das von Sylvester und Stern auf anderem Wege gewonnene Resultat (9) kann bekanntlich vermöge der Identität

$$\sum_{\nu=1}^{2m} c_\nu - 2 \sum_{1}^{m} c_{2\nu} = \sum_{\nu=1}^{2m} (-1)^{\nu-1} c_\nu$$

auf die Gestalt

$$(9') \qquad \frac{2^p - 2}{p} \equiv \sum_{1}^{p-1} (-1)^{\nu-1} \frac{1}{\nu} \pmod{p}$$

gebracht werden.

Eine neue Darstellung des in Rede stehenden Restes fließt aus der Annahme $a = 4$; alsdann spalten sich die Indizes ν in drei Sektionen

$$\left(\frac{p}{4} \cdots \frac{p}{2}\right), \left(\frac{p}{2} \cdots \frac{3p}{4}\right), \left(\frac{3}{4}p \cdots p\right),$$

welchen beziehungsweise die Werte 1, 2, 3 des größten Ganzen $\left[\frac{4\nu}{p}\right]$ entsprechen.

In den Termen der zweiten und dritten Sektion führe ich nun die Substitution $\nu = p - \mu$ aus und beachte, daß alsdann

$$\frac{1}{\nu} = \frac{1}{p-\mu} \equiv -\frac{1}{\mu}$$

ist; es kommt

$$4q(4) \equiv \sum_{\frac{1}{4}p<\nu<\frac{1}{2}p} \frac{1}{\nu} - 2\sum_{\frac{1}{4}p<\mu<\frac{1}{2}p} \frac{1}{\mu} - 3\sum_{1}^{\left[\frac{1}{4}p\right]} \frac{1}{\varrho};$$

die linke Seite ist

$$8q(2) = 4\,\frac{2^p-2}{p},$$

während sich auf der rechten die zwei ersten Aggregate zusammenziehen, so daß man die Kongruenz erhält:

$$4\,\frac{2^p-2}{p} \equiv -\sum_{\left(\frac{1}{4}p<\mu<\frac{1}{2}p,\ 0<\varrho<\frac{p}{4}\right)} \frac{1}{\mu} - 3\sum \frac{1}{\varrho} \pmod{p}.$$

Die Zahlen ϱ ergänzen die Zahlengruppe μ zur Gesamtheit der Zahlen ν des Intervalls $\left(0 \cdots \frac{1}{2}p\right)$, und demnach entsteht, wenn man das eine Aggregat

$$\sum \frac{1}{\varrho}$$

mit dem Aggregat

$$\sum \frac{1}{\mu}$$

vereinigt, die Kongruenz

$$4\,\frac{2^p-2}{p} \equiv -\sum_{1}^{m} \frac{1}{\nu} - 2\sum_{1}^{\left[\frac{1}{4}p\right]} \frac{1}{\varrho};$$

zieht man von hier das Resultat (9) ab, so kommt

$$3\,\frac{2^p-2}{p} \equiv -2\sum_{1}^{\left[\frac{1}{4}p\right]} \frac{1}{\varrho}$$

oder, unter der Annahme $p > 3$,

$$\frac{2^{p-1}-1}{p} \equiv -\frac{1}{3}\sum_{\nu=1}^{\left[\frac{1}{4}p\right]} \frac{1}{\nu} \pmod{p}. \tag{10}$$

Indem wir nochmals auf (9)

$$\sum_{1}^{m} \frac{1}{\nu} \equiv -\frac{2^p-2}{p}$$

zurückgreifen, spalten wir die Zahlen ν in gerade 2μ und ungerade λ, und erhalten

$$\sum_1^m \frac{1}{\nu} = \sum_{\lambda \leq m} \frac{1}{\lambda} + \frac{1}{2} \sum_1^{\left[\frac{p}{4}\right]} \frac{1}{\mu},$$

also mit Rücksicht auf (10)

$$\frac{2^{p-1}-1}{p} \equiv -2 \sum \frac{1}{\lambda} \pmod{p}, \tag{11}$$
$$(\lambda = 1, 3, 5, \cdots;\ \lambda \leqq m).$$

Ähnlich findet man

$$\sum \frac{1}{\lambda'} \equiv \frac{2^{p-1}-1}{p} \pmod{p}, \tag{12}$$
$$(\lambda' = 1, 3, 5, \cdots, p-2).$$

Die Wahl $a = 8$ würde ferner ergeben

$$4\,\frac{2^p-2}{p} \equiv -\sum \frac{1}{a} - \sum \frac{1}{b} \pmod{p} \tag{13}$$
$$\left(0 < a < \frac{p}{8},\quad 0 < b < \frac{3p}{8}\right).$$

Ich notiere schließlich die ähnlich zu gewinnenden Resultate

$$\frac{3^p-3}{p} \equiv -2 \sum_1^{\left[\frac{1}{3}p\right]} \frac{1}{\nu} \pmod{p}, \tag{14}$$

$$\frac{5^p-5}{p} \equiv -2 \sum \frac{1}{a} - 2 \sum \frac{1}{b} \pmod{p} \tag{15}$$
$$\left(0 < a < \frac{p}{5},\quad 0 < b < \frac{2p}{5}\right).$$

Wir kehren nun zu (8) zurück, indem wir nach a von 1 bis $p-1$ summieren; in der so entstandenen Kongruenz

$$\sum_1^{p-1} q(a) \equiv \sum_{\mu=1}^{p-1} \sum_{\nu=1}^{p-1} \frac{1}{\mu\nu}\left[\frac{\mu\nu}{p}\right] \pmod{p}$$

drückt sich die linke Seite vermöge (4), durch den Wilsonschen Quotienten N aus, während die rechte Seite, sich leicht in eine einfache Summe verwandelt.

Bedeutet nämlich $\psi(n)$ die Anzahl der Lösungen der unbestimmten Gleichung

$$\mu\nu = n;\quad (0 < \mu < p,\ 0 < \nu < p),$$

so wird unser Resultat lauten

$$N \equiv \sum_{n=1}^{(p-1)^2} \frac{\psi(n)}{n} \left[\frac{n}{p}\right] \pmod{p}. \tag{16}$$

Die Zahl $\psi(n)$ kann aber einfacher gedeutet werden, wenn man die Bedingungen in die Form

$$n = \mu\nu, \quad 0 < \mu < p, \quad n < p\mu$$

setzt. Denn demnach ist für μ irgend ein Teiler von n zu setzen, der den Ungleichungen

$$\frac{n}{p} < \mu < p$$

genügt, und ν ist als Komplementärteiler unzweideutig bestimmt. Es ist also $\psi(n)$ die Anzahl der Teiler von n, welche innerhalb der Grenzen $\frac{n}{p}$ und p enthalten sind.

Ein viel einfacheres Resultat ergibt sich aus (8), wenn man auf beiden Seiten mit a multipliziert und dann über $a = 1, 2, \cdots, p-1$ summiert; es ergibt sich so

$$\sum_{a=1}^{p-1} a\,q(a) \equiv \frac{1}{2} \pmod{p}. \tag{17}$$

Dabei wird kein anderes neues Hilfsmittel gebraucht als die Gleichung

$$\sum_{a=1}^{p-1} \left[\frac{\nu a}{p}\right] = \sum_{a=1}^{p-1} \frac{a\nu}{p} - \sum_{b=1}^{p-1} \frac{b}{p} = \frac{(\nu-1)(p-1)}{2},$$

die unmittelbar ersichtlich ist.

Die Kongruenz (7) ist übrigens, wie manche andere Sätze, aus dem Spezialsatz

$$q(p-a) \equiv q(a) + \frac{1}{a} \pmod{p}, \tag{6^1}$$

der sich aus (6) vermöge der Identität

$$q(-a) = q(a)$$

ergibt, leicht zu gewinnen.

Wir wollen ferner die Summe

$$S = \sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) q(\nu)$$

betrachten, in welcher der Ausdruck

$$\left(\frac{\nu}{p}\right)$$

in üblicher Weise das aus der Theorie der quadratischen Reste bekannte Legendresche Zeichen ist. Wir machen erstens die Annahme, daß die Primzahl p die Form $4x+3$ hat; alsdann gilt

$$\left(\frac{p-\nu}{p}\right) = -\left(\frac{\nu}{p}\right),$$

und daher verwandelt sich S, wenn man darin $\nu = p-\mu$ setzt, in

$$S = -\sum_{\mu=1}^{p-1}\left(\frac{\mu}{p}\right) q(p-\mu),$$

und dies ist nach (6[1])

$$S \equiv -\sum_{\mu=1}^{p-1}\left(\frac{\mu}{p}\right) q(\mu) - \sum_{\mu=1}^{p-1}\left(\frac{\mu}{p}\right)\frac{1}{\mu} \pmod{p},$$

woraus unmittelbar

$$2S \equiv -\sum_{\mu=1}^{p-1}\left(\frac{\mu}{p}\right)\frac{1}{\mu} \pmod{p}$$

folgt. Die Eulersche Kongruenz

$$\left(\frac{\mu}{p}\right) \equiv \mu^m \pmod{p}; \quad m = \frac{p-1}{2},$$

gestattet unsere letzte Kongruenz wie folgt zu schreiben:

$$2S \equiv -\sum_{\mu=1}^{p-1}\mu^{m-1} \pmod{p}.$$

Nun ist nach der bekannten Formel der Differenzenrechnung

$$u_0 + u_1 + \cdots + u_{n-1} = \sum_{\nu=0}^{n-1}\binom{n}{\nu+1}\Delta^\nu u_0,$$

also für

$$u_\nu = \nu^{m-1}, \quad n = p$$

$$\sum_{1}^{p-1}\mu^{m-1} = \sum_{\nu=0}^{p-1}\binom{p}{\nu+1}\Delta^\nu 0^{m-1} = \sum_{\nu=0}^{m-1}\binom{p}{\nu+1}\Delta^\nu 0^{m-1},$$

weil die m^{te} und die höheren Differenzen der $(m-1)^{\text{ten}}$ Potenzen natürlicher Zahlen sämtlich verschwinden. Hier ist nun jeder vorkommende Binomialkoeffizient

$$\binom{p}{\nu+1}$$

durch p teilbar, also

$$\sum \mu^{m-1} \equiv 0 \pmod{p}.$$

Demnach ist

$$S \equiv 0 \pmod{p},$$

d. h.

$$\sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) q(\nu) \equiv 0 \pmod{p}, \tag{18}$$

falls die Primzahl p die Gestalt $4x+3$ hat.

Für Primzahlen der Gestalt $4x+1$ versagt die obige Betrachtung, und wir müssen uns nach anderen Hilfsmitteln umsehen, um den Rest der Summe S zu ermitteln.

Wegen der Eulerschen Kongruenz

$$\nu^m \equiv \left(\frac{\nu}{p}\right) \pmod{p}$$

ist die durch die Gleichung

$$\nu^m = \left(\frac{\nu}{p}\right)[1 + pq'(\nu)] \tag{19}$$

definierte Zahl $q'(\nu)$ eine ganze Zahl; dieselbe steht mit der Zahl $q(\nu)$ im engen Zusammenhange, und zwar ist, wie sich durch Quadrieren von (19) ergibt

$$1 + 2pq'(\nu) + p^2 q'(\nu)^2 = 1 + pq(\nu),$$

also

$$q(\nu) = 2q'(\nu) + pq'(\nu)^2, \tag{20}$$

woraus

$$q(\nu) \equiv 2q'(\nu) \pmod{p}. \tag{20^0}$$

Ich setze nun für p eine Primzahl $4n+1$, so daß $m = 2n$ gerade ist, und bilde die Summe der Zahlen (19) für $\nu = 1, 2, \cdots, p-1$. Mit Rücksicht auf die Relation

$$\sum_{1}^{p-1} \left(\frac{\nu}{p}\right) = 0$$

ergibt sich in der Weise die Gleichung

$$\sum_{\nu=1}^{p-1} \nu^m = p \sum_{1}^{p-1} \left(\frac{\nu}{p}\right) q'(\nu).$$

Hier läßt sich die linke Seite mit Hilfe der bekannten Formel

$$S_{2n}(x) = \frac{x^{2n+1}}{2n+1} - \frac{1}{2} x^{2n} + \sum_{\nu=1}^{n} (-1)^{\nu-1} \frac{B_\nu}{2\nu} \binom{2n}{2\nu-1} x^{2n-2\nu+1}$$

ausdrücken, und zwar ist

$$\sum_{\nu=1}^{p-1} \nu^m = S_{2n}(p), \quad 2n = m.$$

Wir erhalten daher

$$\sum_{\nu=1}^{n} (-1)^{\nu-1} \frac{B_\nu}{2\nu} \binom{2n}{2\nu-1} p^{2n-2\nu} + \frac{p^m}{m+1} - \frac{1}{2} p^{m-1} = \sum_{1}^{p-1} \left(\frac{\nu}{p}\right) q'(\nu).$$

Links enthält keine der auftretenden Bernoullischen Zahlen B_ν den Faktor p im Nenner, und daher läßt sich hieraus die Kongruenz

$$(-1)^{n+1} B_n \equiv \sum_{1}^{p-1} \left(\frac{\nu}{p}\right) q'(\nu) \pmod{p}$$

erschließen; *dieselbe geht aber nach* (20⁰) *über in*

$$S = \sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) q(\nu) \equiv (-1)^{n-1} 2 B_n \pmod{p}, \tag{21}$$

wobei die Primzahl $p = 4n + 1$ *ist.*

Wir wollen ferner die Summe

$$H = \sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) \nu q(\nu) \tag{22}$$

nach dem Modul p abschätzen.

Ist zunächst p der Gestalt $4x + 1$, so wird

$$\left(\frac{p-a}{p}\right) = \left(\frac{a}{p}\right),$$

und wenn wir mit a Zahlen $\leqq m$ bezeichnen, so zerfallen die $p-1$ Zahlen ν in die Zahlen a und $p-a$, so daß

$$H = \sum \left(\frac{a}{p}\right) a q(a) + \sum \left(\frac{p-a}{p}\right) (p-a) q(p-a)$$

also

$$H \equiv \sum \left(\frac{a}{p}\right) a [q(a) - q(p-a)] \pmod{p}$$

ist. Die Klammer ist aber nach (6¹) der Zahl

$$-\frac{1}{a}$$

kongruent, und *wir erhalten*

$$H \equiv -\sum_{a=1}^{m} \left(\frac{a}{p}\right) = 0,$$

also

$$(22^1) \qquad \sum_{\nu=1}^{p-1} \left(\frac{\nu}{p}\right) \nu q(\nu) \equiv 0 \pmod{p},$$

wenn $p = 4x + 1$.

Wenn dagegen $p = 4x + 3$ ist, so ergibt die Spaltung der Zahlen ν in a und $p - a$ zunächst

$$H = \sum \left(\frac{a}{p}\right) a q(a) + \sum \left(\frac{p-a}{p}\right) (p-a) q(p-a)$$

und also

$$(\gamma) \qquad H \equiv 2 \sum \left(\frac{a}{p}\right) a q(a) + \sum \left(\frac{a}{p}\right) \pmod{p}.$$

Ferner lassen sich die Zahlen ν in gerade $2a$ und ungerade $p - 2a$ spalten; die Summe H nimmt dadurch die Gestalt an

$$H = \sum \left(\frac{2a}{p}\right) 2a q(2a) + \sum \left(\frac{p-2a}{p}\right) (p-2a) q(p-2a),$$

also

$$H \equiv 4 \sum \left(\frac{2a}{p}\right) a q(2a) + \sum \left(\frac{2a}{p}\right) \pmod{p}.$$

Wegen

$$q(2a) \equiv q(a) + q(2)$$

läßt sich dies schreiben

$$H \equiv 4 \left(\frac{2}{p}\right) \sum \left(\frac{a}{p}\right) a q(a) + \left(\frac{2}{p}\right) \sum \left(\frac{a}{p}\right) + 4 \left(\frac{2}{p}\right) q(2) \sum \left(\frac{a}{p}\right) a.$$

Die Summe

$$\sum \left(\frac{a}{p}\right) a$$

hat eine aus der Theorie der quadratischen Formen bekannte Bedeutung; für uns kommt sie jedoch in Wegfall, weil sie durch p teilbar ist, und wir haben daher

$$(\delta) \qquad H \equiv 4 \left(\frac{2}{p}\right) \sum \left(\frac{a}{p}\right) a q(a) + \left(\frac{2}{p}\right) \sum \left(\frac{a}{p}\right).$$

Multiplizieren wir nun (γ) mit 2, (δ) mit $\left(\frac{2}{p}\right)$ und ziehen ab, so entsteht

$$\left(2 - \left(\frac{2}{p}\right)\right) H \equiv \sum \left(\frac{a}{p}\right) \pmod{p}.$$

Nun ist aber nach bekannten Sätzen von Dirichlet

$$\sum_{a=1}^{m} \left(\frac{a}{p}\right) = \left(2 - \left(\frac{2}{p}\right)\right) Cl(-p),$$

wenn mit $Cl(-\Delta)$ die Anzahl primitiver positiver Klassen quadratischer

Formen $ax^2+bxy+cy^2$ der negativen Diskriminante $b^2-4ac=-\Delta$ bezeichnet wird, und *also lautet unser Resultat*

$$H\equiv Cl(-p) \pmod p,$$

d. h.

$$(22^2) \qquad \sum_{\nu=1}^{p-1}\left(\frac{\nu}{p}\right)\nu q(\nu)\equiv Cl(-p) \pmod p,$$

wenn die Primzahl p die Form $4x+3$ hat.

Wir gehen nun auf die oben betrachtete Summe

$$(23) \qquad A=\sum_{\nu=1}^{p-1}\left(\frac{\nu}{p}\right)q(\nu)$$

zurück. Die Kongruenz (7) oder

$$(7') \qquad q(\nu b)\equiv q(\varrho)-\frac{1}{\nu b}\left[\frac{\nu b}{p}\right],$$

wenn $0<\varrho<p$, $\nu b\equiv\varrho \pmod p$, verbunden mit dem Umstande, daß

$$\left(\frac{\nu b}{p}\right)=\left(\frac{\varrho}{p}\right),$$

liefert nach dem Satze $q(\nu b)\equiv q(\nu)+q(b)$ offenbar

$$\left(\frac{b}{p}\right)\left(\frac{\nu}{p}\right)q(\nu)+\left(\frac{b}{p}\right)q(b)\left(\frac{\nu}{p}\right)\equiv\left(\frac{\varrho}{p}\right)q(\varrho)-\left(\frac{\nu b}{p}\right)\frac{1}{\nu b}\left[\frac{\nu b}{p}\right] \pmod p.$$

Summiert man hier über die Werte $\nu=1,2,\cdots,p-1$, so nimmt ϱ die gleichen Werte an, und es kommt

$$\left(\frac{b}{p}\right)A\equiv A-\sum_{\nu=1}^{p-1}\left(\frac{b\nu}{p}\right)\left[\frac{b\nu}{p}\right]\frac{1}{b\nu} \pmod p$$

oder nach Kürzen durch $\left(\frac{b}{p}\right)$

$$(23^*) \qquad \sum_{\nu=1}^{p-1}\left(\frac{\nu}{p}\right)\left[\frac{b\nu}{p}\right]\frac{1}{\nu}\equiv-\left(1-\left(\frac{b}{p}\right)\right)bA \pmod p.$$

Wenn also b quadratischer Rest von p ist, so ist die Summe

$$\sum_{\nu=1}^{p-1}\left(\frac{\nu}{p}\right)\left[\frac{b\nu}{p}\right]\frac{1}{\nu}$$

durch p teilbar; sie ist es auch dann, wenn p die Gestalt $4n+3$ hat; ist dagegen p der Gestalt $4n+1$ und ist b ein Nichtrest von p, so ist unsere Summe nach dem Modul p der Zahl

$$(-1)^n 4B_n b$$

kongruent, wobei B_n wie oben in (21) die n^{te} Bernoullische Zahl bedeutet.

Die Kongruenz (7′) ergibt, wenn man sie mit

$$b^2\nu^2 \equiv \varrho^2$$

multipliziert, die folgende

$$b^2 q(b)\cdot\nu^2 + b^2\cdot\nu^2 q(\nu) \equiv \varrho^2 q(\varrho) - b\nu\left[\frac{b\nu}{p}\right].$$

Wenn man hier über $\nu = 1, 2, \cdots, p-1$ summiert und beachtet, daß

$$\sum \nu^2 \equiv 0 \pmod{p},$$

so kommt

$$(\varepsilon)\qquad (b^2-1)\sum_{\nu=1}^{p-1}\nu^2 q(\nu) \equiv -b\sum_{\nu=1}^{p-1}\nu\left[\frac{b\nu}{p}\right] \pmod{p}.$$

Setzt man hier $b = 2$, so entsteht

$$3\sum \nu^2 q(\nu) \equiv -2\sum_{\nu=m+1}^{p-1}\nu = -2\left(\sum_{1}^{p-1}\nu - \sum_{1}^{m}\nu\right),$$

also

$$3\sum \nu^2 q(\nu) \equiv m(m+1) = \frac{p^2-1}{4} \equiv -\frac{1}{4};$$

dies gibt einerseits das Resultat

$$(24)\qquad \sum_{\nu=1}^{p-1}\nu^2 q(\nu) \equiv -\frac{1}{12} \pmod{p},$$

andererseits, wenn man dies in (ε) einsetzt, die interessante Kongruenz

$$(25)\qquad \sum_{\nu=1}^{p-1}\nu\left[\frac{b\nu}{p}\right] \equiv \frac{b^2-1}{12b} \pmod{p}.$$

Dieselbe liefert eine Darstellung der Zahl $\frac{1}{a} \pmod{p}$, in welcher die Zahl a nur „ganzen“ Operationen unterworfen wird, nämlich

$$(25^*)\qquad \frac{1}{a} \equiv a - 12\sum_{\nu=1}^{p-1}\nu\left[\frac{a\nu}{p}\right] \pmod{p}.$$

Dadurch wird auch für die unbestimmte Gleichung

$$ax - py = 1$$

eine Lösung

$$x = a - 12\sum_{\nu=1}^{p-1}\nu\left[\frac{a\nu}{p}\right]$$

gefunden, jedoch nur für den Fall, daß p eine Primzahl ist.

Diese Anwendung der Theorie Fermatscher Quotienten macht das Bedürfnis dringend, den Begriff der Zahlen $q(a)$ auf *zusammengesetzte Moduln* zu erweitern. Es sei also m ein ungerader Modul, $\varphi(m)$ die Anzahl der Zahlen, die kleiner als m und ohne gemeinsamen Teiler mit m sind; ist a zu m relativ prim, so besteht die Kongruenz

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

und demnach ist die durch die Gleichung

$$a^{\varphi(m)} = 1 + mq(a) \tag{26}$$

bestimmte Zahl $q(a)$ ganz.

Man findet leicht die Gesetze

$$\begin{cases} q(ab) \equiv q(a) + q(b) \pmod{m}, \\ q(c+mz) \equiv q(c) + \frac{\varphi(m)z}{c} \pmod{m}; \end{cases} \tag{27}$$

aus der zweiten läßt sich für $ab \equiv c \pmod{m}$, und $0 < c < m$ die weitere Kongruenz

$$q(ab) \equiv q(c) + \frac{\varphi(m)}{ab}\left[\frac{ab}{m}\right] \pmod{m} \tag{28}$$

ableiten. Multiplizieren wir beiderseits mit $a^2b^2 \equiv c^2$, und schreiben $q(a) + q(b)$ an Stelle von $q(ab)$, so kommt

$$a^2q(a) \cdot b^2 + a^2b^2q(b) \equiv c^2q(c) + \varphi(m)\, ab\left[\frac{ab}{m}\right].$$

Hier lassen wir b die sämtlichen $\varphi(m)$ zum Modul relativ primen Zahlen durchlaufen und addieren die Resultate; da alsdann c dieselben Zahlen wie b durchläuft, so entsteht

$$(\eta) \qquad a^2q(a)s_2 + (a^2-1)\sum_b{}' b^2q(b) \equiv \varphi(m)\, a \sum_b{}' b\left[\frac{ab}{m}\right] \pmod{m},$$

wobei s_2 die Summe der Quadrate der zum Modul relativ primen Zahlen bedeutet.

Setzt man hier zunächst $a = 2$, so kommt

$$(\xi) \qquad 4q(2)s_2 + 3\sum{}' b^2q(b) \equiv 2\varphi(m) \sum{}' b' \pmod{m},$$

wobei in der letzten Summation die Bedingung

$$b' > \frac{m}{2}$$

zu erfüllen ist.

Nun ist aber

$$\sum{}' b' \equiv -\sum{}' \beta \pmod{m},$$

wenn β die relativen Primzahlen von m, welche zwischen 0 und $\frac{m}{2}$ liegen durchläuft.

Bedeutet

$$f(n) = \sum_{\nu=1}^{\left[\frac{n}{2}\right]} \nu,$$

so ist

$$\sum \beta = \sum \mu(d)\, df\left(\frac{m}{d}\right),$$

wobei d die sämtlichen Teiler von m durchläuft und $\mu(d)$ die übliche Bezeichnung für die Moebiusschen Zahlen ist. Da m, also auch $\frac{m}{d} = d'$, ungerade ist, so hat man

$$f(d') = \sum_{1}^{\frac{d'-1}{2}} \nu = \frac{d'^2-1}{8},$$

also

$$\sum \beta = \frac{1}{8} \sum \mu(d)\,(md'-d). \tag{29}$$

Hieraus folgt

$$\sum \beta \equiv -\frac{1}{8} \sum d\,\mu(d),$$

also, wenn die Bezeichnung eingeführt wird

$$P(m) = (1-p)\,(1-p')\,(1-p'')\cdots, \tag{30}$$

wobei $p, p', p'', \cdots$ die verschiedenen Primfaktoren des Moduls m bedeuten,

$$\sum \beta \equiv -\frac{1}{8} P(m) \pmod{m}. \tag{31}$$

Ferner ist die Zahl s_2 zu ermitteln. Setzt man der Kürze wegen

$$F(n) = \sum_{1}^{n-1} \nu^2,$$

so wird

$$s_2 = \sum_{d} \mu(d)\, d^2 F\left(\frac{m}{d}\right),$$

wobei wieder d die sämtlichen Teiler von m anzunehmen hat.

Nun ist bekanntlich

$$F(n) = \frac{n^3}{3} - \frac{n^2}{2} + \frac{n}{6},$$

und daher

$$s_2 = \frac{m^2}{3} \sum \mu(d)\, d' - \frac{m^2}{2} \sum \mu(d) + \frac{m}{6} \sum d\,\mu(d),$$

oder da $\sum \mu(d) = 0$,

$$s_2 = \frac{m^2}{3} \varphi(m) + \frac{m}{6} P(m). \tag{32}$$

Ist nun m durch 3 nicht teilbar, so folgt aus (32)

$$s_2 \equiv 0 \pmod{m}$$

und das Resultat (ξ) lautet

$$\sum b^2 q(b) \equiv \frac{1}{12}\varphi(m) P(m) \pmod{m}, \tag{33}$$

wobei links die Summation sich über alle die $\varphi(m)$ zu m teilerfremden Zahlen b zwischen Null und m erstreckt.

Setzt man dies in (η) ein, so kommt zunächst

$$\left(a - \frac{1}{a}\right)\frac{\varphi(m) P(m)}{12} \equiv \varphi(m) \sum_b b\left[\frac{ab}{m}\right].$$

Diese Kongruenz führt zu einem einfachen Resultate, wenn die Zahl $\varphi(m)$ zu m prim ist; dies findet statt, wenn m das Produkt von lauter verschiedenen Primzahlen ist, falls überdies das Produkt $P(m)$ durch keine derselben aufgeht. Alsdann wird man durch $\varphi(m)\ P(m)$ dividieren dürfen, und *es kommt*

$$\frac{1}{a} \equiv a - \frac{12}{P(m)} \sum_b b\left[\frac{ab}{m}\right] \pmod{m}, \tag{34}$$

wobei sich die Bedingung am bequemsten durch

$$(m, \varphi(m)) \sim 1 \tag{35}$$

ausdrückt, und die Summation sich über die $\varphi(m)$ relativen Primzahlen b von m des Intervalls $(0 \cdots m)$ erstreckt.

Ist dagegen m durch 3 teilbar, und sollen die Zahlen m und $\varphi(m)$ relativ prim sein, so wird keine der Differenzen $p - 1$ durch 3 aufgehen, also werden die sämtlichen Primfaktoren von m außer 3 die Form $3x + 2$ haben. Alsdann ist

$$s_2 \equiv \frac{m}{6} P(m),$$

und es folgt aus (ξ)

$$3\sum b^2 q(b) \equiv P(m)\left[\frac{1}{4}\varphi(m) - \frac{2}{3} m q(2)\right] \pmod{m}.$$

Die Kongruenz (η) kann alsdann unter die Form gebracht werden

$$\frac{a^2-1}{3} P(m)\left[\frac{1}{4}\varphi(m) - \frac{2}{3} m q(2)\right] + a^2 q(a) \cdot \frac{m}{6} P(m) \equiv \varphi(m) a \sum b\left[\frac{ab}{m}\right] \pmod{m}.$$

Multipliziert man mit 3, so fällt das zweite Glied links heraus, und das Glied

$$(a^2-1)\ P(m)\ \frac{2}{3} m q(2)$$

wird durch m teilbar sein, da $a^2 - 1$ durch 3 aufgeht. Demnach entsteht

$$\left(a - \frac{1}{a}\right) \frac{P(m)\,\varphi(m)}{4} \equiv \varphi(m) \cdot 3 \sum b \left[\frac{ab}{m}\right],$$

und hieraus wieder die Kongruenz (34).

Dieselbe ist daher bloß an die Bedingung

$$(m,\ \varphi(m)) \sim 1$$

gebunden.

Die Moduln m, welche die Bedingung (35) erfüllen, haben überhaupt die Eigenschaft, daß man auf sie die Theorie der Quotienten $q(a)$ ausdehnen kann. Namentlich erhält man analog wie im Falle des Primzahlmoduls

$$q(a) \equiv \sum_{\nu} \frac{1}{a\nu} \left[\frac{a\nu}{m}\right] \pmod{m}, \tag{36}$$

wobei ν die zu m relativen Primzahlen des Intervalls $(0 \cdots m)$ durchläuft. Speziell folgt hieraus eine Verallgemeinerung der Sylvesterschen Kongruenz (9)

$$2\,\frac{2^{\varphi(m)} - 1}{m} \equiv \sum{}^{*} \frac{1}{\nu} \equiv -\sum{}^{*} \frac{1}{\mu} \pmod{m}$$

$$\left(\frac{m}{2} < \nu < m;\ \ 0 < \mu < \frac{m}{2}\right),$$

wobei selbstverständlich ν und μ relativ prim zum Modul sein müssen.

Wir kehren zum einfacheren Falle des Primzahlmoduls p wieder zurück und betrachten die quadratischen Reste r des Moduls p. Werden dieselben in den Grenzen $0 \cdots p$ angenommen, so sind sie durch die Kongruenzen

$$\nu^2 \equiv r \pmod{p}$$

vollständig charakterisiert, und zwar wird jede der $\frac{p-1}{2}$ Zahlen r zweimal erzeugt, wenn ν die sämtlichen Werte 1 bis $p - 1$ annimmt. Die Kongruenz (7) ergibt

$$q(\nu^2) \equiv q(r) - \left[\frac{\nu^2}{p}\right] \frac{1}{\nu^2};$$

summiert man über die sämtlichen ν von 1 bis $p - 1$, und beachtet, daß

$$q(\nu^2) \equiv 2q(\nu),$$

so entsteht

$$2 \sum_{\nu=1}^{p-1} q(\nu) \equiv 2 \sum_{r} q(r) - \sum_{\nu=1}^{p-1} \frac{1}{\nu^2} \left[\frac{\nu^2}{p}\right] \pmod{p}.$$

Nun ist

$$\sum q(\nu) \equiv N,$$

ferner identisch

$$2\sum_r q(r) = \sum\left(1+\left(\frac{\nu}{p}\right)\right)q(\nu),$$

also mit Benützung der Notation (23)

$$2\sum_r q(r) \equiv N + A,$$

und unser Resultat läßt sich schreiben

$$\sum_{\nu=1}^{p-1}\frac{1}{\nu^2}\left[\frac{\nu^2}{p}\right] \equiv A - N \pmod{p}. \tag{37}$$

Ist speziell $p = 4n+3$, so ist nach (18)

$$A \equiv 0$$

und die Kongruenz gibt eine *bemerkenswerte Darstellung des Restes des Wilsonschen Quotienten N.*

Ich werde bei einer anderen Gelegenheit zeigen, daß sich für jede ungerade Primzahl p der Wilsonsche Quotient N nach dem Modul p durch eine Bernoullische Zahl ausdrücken läßt, nämlich bei der früheren Bezeichnung $p = 2m+1$

$$N \equiv -1 + \frac{1}{p} - (-1)^m B_m \pmod{p}.$$

Im Falle $p = 4n+1$ haben wir oben (21) gefunden, daß

$$A \equiv (-1)^{n-1} 2B_n \pmod{p},$$

und da hier

$$N \equiv -1 + \frac{1}{p} - B_{2n},$$

so lautet (37) für $p = 4n+1$ wie folgt:

$$\sum_1^{p-1}\frac{1}{\nu^2}\left[\frac{\nu^2}{p}\right] \equiv 1 - (-1)^n 2B_n + B_{2n} - \frac{1}{p} \pmod{p}. \tag{37^1}$$

Die bisher angewandte Schlußweise ließe noch weitere Anwendungen zu; wir wollen jedoch den Gegenstand verlassen, und schließen mit einigen ähnlichen Formeln, in welchen sich nun die Summationen entweder über die quadratischen Reste oder über die Nichtreste des Moduls erstrecken.

Wir bezeichnen mit a oder $a', a'', \cdots$ quadratische Reste, mit b, resp. $b', b'', \cdots$ Nichtreste von p und setzen

$$\sum_a q(a) = A, \quad \sum_b q(b) = B.$$

Nach (7) ist

$$aa' \equiv a' + pz, \quad z = \left[\frac{aa'}{p}\right],$$

$$q(aa') \equiv q(a'') - \frac{1}{aa'}\left[\frac{aa'}{p}\right] \equiv q(a) + q(a').$$

Summiert man über die a', so durchläuft a'' die gleichen Werte und es kommt

$$mq(a) \equiv -\sum_{a'} \frac{1}{aa'}\left[\frac{aa'}{p}\right]$$

oder

$$q(a) \equiv 2\sum_{a'} \frac{1}{aa'}\left[\frac{aa'}{p}\right], \tag{38}$$

wobei die Summation sich über die sämtlichen quadratischen Reste a' des Moduls p erstreckt, letztere natürlich in den Grenzen 0 und p vorausgesetzt.

Ferner ist bei der angenommenen Bezeichnung

$$ab \equiv b' \pmod{p},$$

also

$$ab \equiv b' + pz$$

und

$$q(ab) \equiv q(b') - \frac{1}{ab}\left[\frac{ab}{p}\right] \equiv q(a) + q(b). \tag{a}$$

Wird hier über die sämtlichen m Werte b summiert, so entsteht

$$mq(a) \equiv -\sum_{b} \frac{1}{ab}\left[\frac{ab}{p}\right],$$

oder

$$q(a) \equiv 2\sum_{b} \frac{1}{ab}\left[\frac{ab}{p}\right] \pmod{p}. \tag{38^1}$$

Diese beiden Sätze (38) und (38^1) sind übrigens eine direkte Folge der Sätze (8) und (23*).

Wird dagegen in (a) über die m Werte a summiert, so entsteht

$$mq(b) + A \equiv B - \sum_{a} \frac{1}{ab}\left[\frac{ab}{p}\right]$$

oder

$$q(b) \equiv 2A - 2B + 2\sum_{a} \frac{1}{ab}\left[\frac{ab}{p}\right] \pmod{p}. \tag{39}$$

Ferner ist

$$bb' = a + pz$$

und demnach

$$q(b) + q(b') \equiv q(a) - \frac{1}{bb'}\left[\frac{bb'}{p}\right];$$

wird hier über die b' summiert, so entsteht

$$mq(b) + B \equiv A - \sum_{b'} \frac{1}{bb'} \left[\frac{bb'}{p}\right]$$

oder

$$q(b) \equiv -2A + 2B + 2 \sum_{b'} \frac{1}{bb'} \left[\frac{bb'}{p}\right] \pmod{p}. \tag{39'}$$

Vergleicht man dies mit (39), so entsteht

$$\sum_{a} \frac{1}{ab} \left[\frac{ab}{p}\right] - \sum_{b'} \frac{1}{bb'} \left[\frac{bb'}{p}\right] \equiv 2(A-B) \pmod{p},$$

ein Resultat, das in (23*) enthalten ist; denn hier bedeutet b einen Nichtrest, also

$$\left(\frac{b}{p}\right) = -1,$$

und der Buchstabe A in (23*) ist

$$\sum_{1}^{p-1} \left(\frac{v}{p}\right) q(v),$$

fällt also mit unserem jetzigen $A - B$ zusammen.