Werk

Titel: Journal für die reine und angewandte Mathematik
Verlag: de Gruyter
Jahr: 1913
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN243919689_0142
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN243919689_0142

LOG Id: LOG_0005
LOG Titel: Über den Rest von ... (mod.p).
LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN243919689
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN243919689

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Über den Rest von $\frac{2^{p-1}-1}{p}$ (mod. p).

Von Herrn *P. Bachmann* in Weimar.

1. Die Bedingung, welche Herr *Wieferich* für die Auflösbarkeit der Gleichung

$$x^p + y^p + z^p = 0,$$

wo p eine ungerade Primzahl bedeutet, in ganzen durch p nicht teilbaren Zahlen x, y, z als erforderlich nachgewiesen hat (dieses Journ., Bd. 136), hat die Aufmerksamkeit wieder auf die Frage nach dem Reste gelenkt, den der Ausdruck

$$(1.) \qquad \frac{2^{p-1}-1}{p}$$

(mod. p) läßt, eine Frage, welche u. a. bereits von *Stern* (ebend. Bd. 100, S. 182; vgl. des Verf. Niedere Zahlentheorie I, S. 159 ff.) behandelt worden ist. Ihm zufolge bestimmt sich dieser Rest durch die Kongruenz

$$(2.) \qquad \frac{2^{p-1}-1}{p} \equiv 1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p-2} \pmod{p},$$

in welcher $\frac{1}{u}$ den Sozius von u (mod. p) bedeutet, so daß man kürzer, diesen letzteren durch u' bezeichnend, schreiben darf

$$(3.) \qquad \frac{2^{p-1}-1}{p} \equiv \sum_u u' \pmod{p},$$

wenn die Summation auf alle ungeraden Zahlen u der Reihe $1, 2, 3, \ldots p-1$ erstreckt wird. Am einfachsten gewinnt man diese Formel durch binomische Entwicklung aus der Gleichung

$$2^p = (1+1)^p - (1-1)^p,$$

was

$$2^p - 2 = 2 \cdot \left[\binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{p-2}\right]$$

ergibt und nach Division mit $2p$ und Vernachlässigung von Vielfachen von p sogleich zur Formel (2.) hinführt. Wir leiten sie zunächst aus einer anderen, wohl noch nicht benutzten Quelle hier ab. Es sei, unter a, b, c beliebige Zahlen verstanden,

$$(4.)\quad S=(a+b+c)^p-(a+b-c)^p-(a-b+c)^p-(-a+b+c)^p.$$

Mit Beachtung der Formel

$$(m+n)^p-(m-n)^p$$
$$=2\left[\binom{p}{1}m^{p-1}n+\binom{p}{3}m^{p-3}n^3+\cdots+\binom{p}{p-2}m^2n^{p-2}+n^p\right]$$

läßt sich S in folgender Weise darstellen:

$$(5.)\quad S=2\left[\binom{p}{1}\cdot c[(a+b)^{p-1}-(a-b)^{p-1}]+\binom{p}{3}\cdot c^3[(a+b)^{p-3}-(a-b)^{p-3}]\right.$$
$$\left.+\cdots+\binom{p}{p-2}\cdot c^{p-2}[(a+b)^2-(a-b)^2]\right].$$

Aus dieser allgemeinen Formel erhält man für $a=b=1$, $c=2$ die besondere:

$$2^{p+1}\cdot\frac{2^{p-1}-1}{p}$$
$$=2\cdot\left[2\cdot2^{p-1}+\frac{(p-1)(p-2)}{1\cdot2\cdot3}\cdot2^3\cdot2^{p-3}+\frac{(p-1)(p-2)(p-3)(p-4)}{1\cdot2\cdot3\cdot4\cdot5}\cdot2^5\cdot2^{p-5}\right.$$
$$\left.+\cdots+\frac{(p-1)(p-2)\cdots3}{1\cdot2\cdot3\cdots(p-2)}\cdot2^{p-2}\cdot2^2\right]$$

oder, wenn mit 2^{p+1} geteilt wird und zur Rechten nur die Reste (mod. p) genommen werden, wieder die gedachte Formel (2.). Setzt man dagegen $a=b=c=1$, so entsteht die Beziehung

$$\frac{3^p-3}{p}$$
$$=2\cdot\left[2^{p-1}+\frac{(p-1)(p-2)}{1\cdot2\cdot3}2^{p-3}+\frac{(p-1)(p-2)(p-3)(p-4)}{1\cdot2\cdot3\cdot4\cdot5}\cdot2^{p-5}+\cdots\right.$$
$$\left.+\frac{(p-1)(p-2)\cdots3}{1\cdot2\cdot3\cdots(p-2)}\cdot2^2\right]$$

und hieraus die, soviel ich weiß, noch nicht angegebene Kongruenz

$$(6.)\quad\frac{3^p-3}{p}\equiv2\left[\frac{2^{p-1}}{1}+\frac{2^{p-3}}{3}+\frac{2^{p-5}}{5}+\cdots+\frac{2^2}{p-2}\right]\ (\text{mod. }p),$$

welcher nach Herrn *Mirimanoff*s Mitteilung in den Comptes Rendus de l'Ac. des Sciences, Paris, 1910 (vgl. auch dieses Journ., Bd. 139, S. 309) für die Auflösbarkeit der *Fermat*schen Gleichung dieselbe Bedeutung zukommt, wie der Kongruenz (2.).

Die letztere kann übrigens auch durch die folgende ersetzt werden:

$$(7.)\quad\frac{2^p-2}{p}\equiv1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots+\frac{1}{p-2}-\frac{1}{p-1}\ (\text{mod. }p).$$

Diese gewinnt man unmittelbar und ganz analog wie (2.) und (6.) aus der binomischen Entwicklung der Gleichung

$$2^p = (1+1)^p.$$

Auf demselben Wege kommt

$$3^p = (2+1)^p = 2^p + \binom{p}{1}2^{p-1} + \binom{p}{2}2^{p-2} + \cdots + \binom{p}{p-1}\cdot 2 + 1,$$

mithin

$$\frac{3^p-3}{p} \equiv \frac{2^p-2}{p} + 2^{p-1} - \frac{1}{2}\cdot 2^{p-2} + \frac{1}{3}\cdot 2^{p-3} \cdots - \frac{1}{p-1}\cdot 2 \pmod{p}.$$

Aus dieser Beziehung zwischen den beiden Quotienten $\frac{2^p-2}{p}$, $\frac{3^p-3}{p}$ leitet man mit Rücksicht auf (6.) noch einen neuen Ausdruck zur Restbestimmung des ersteren her, nämlich folgende Formel:

(8.) $$\frac{2^p-2}{p} \equiv 2^{p-1} + \frac{1}{2}\cdot 2^{p-2} + \frac{1}{3}\cdot 2^{p-3} + \cdots + \frac{1}{p-2}\cdot 2^2 + \frac{1}{p-1}\cdot 2 \pmod{p}.$$

2. Aber alle diese eleganten Formeln bieten keine rechte Handhabe dar, um zu entscheiden, ob oder wann die gedachten Quotienten durch p teilbar sind. Man wird daher dazu geführt, andere Ausdrücke aufzusuchen, welche vielleicht dazu geeigneter sind. Ich habe versucht, den bereits auch sonst schon gegebenen einen neuen hinzuzufügen, und teile hier mit, was ich bisher gefunden.

Man teile in der Kongruenz (2.) die Zahlen u in die α Zahlen v, deren Sozius v' ebenfalls ungerade, und in die β Zahlen w, deren Sozius w' gerade ist, so daß, wenn $p - w' = v_1$ gesetzt wird, v_1 eine der Zahlen u und $wv_1 \equiv -1 \pmod{p}$ ist. Sowohl die Zahlen v' als auch die Zahlen v_1 sind untereinander verschieden, aber auch die v_1 von den v', denn, wäre ein v_1 gleich einem der v', so folgte eine Kongruenz $(v+w)v' \equiv 0$, welche unmöglich ist, da $v+w<2p$ und gerade, also von p verschieden ist. Hieraus ergeben sich die Produkte

$$\Pi v \cdot \Pi w = \Pi v' \cdot \Pi v_1 = 1\cdot 3\cdot 5\cdots(p-2)$$

und aus den Kongruenzen $vv' \equiv 1$, $wv_1 \equiv -1$ die andere:

$$[1\cdot 3\cdot 5\cdots(p-2)]^2 \equiv (-1)^\beta \pmod{p},$$

welcher die Form

$$2^{p-1}\cdot\left(1\cdot 2\cdot 3\cdots\frac{p-1}{2}\right)^2 \equiv (-1)^\beta$$

oder, da bekanntlich

$$\left(1\cdot 2\cdot 3\cdots\frac{p-1}{2}\right)^2 \equiv (-1)^{\frac{p+1}{2}}$$

ist, die Form

$$(-1)^{\frac{p+1}{2}} \equiv (-1)^{\beta} \pmod{p}$$

gegeben werden kann. Daraus folgt $\beta \equiv \frac{p+1}{2} \pmod 2$; da aber $\alpha + \beta = \frac{p-1}{2}$ ist, ergibt sich $\alpha \equiv 1 \pmod 2$, d. i. als eine *ungerade* Zahl, während β gerade oder ungerade ist, je nachdem $p \equiv 3$ oder $\equiv 1 \pmod 4$ ist.

Ferner ist

$$\frac{2^{p-1}-1}{p} \equiv \Sigma v' + \Sigma w' \equiv \Sigma v' - \Sigma v_1 \pmod{p},$$

und da

$$\Sigma v' + \Sigma v_1 = 1 + 3 + 5 + \cdots + (p-2) = \left(\frac{p-1}{2}\right)^2$$

ist, findet sich die Kongruenz

$$(9.) \qquad \frac{2^{p-1}-1}{p} + \left(\frac{p-1}{2}\right)^2 \equiv 2 \cdot \Sigma v' \pmod{p}.$$

Die Zahlen v' stimmen insgesamt mit den Zahlen v überein, denn sonst gehörte ein v' zu den Zahlen w, und sein Sozius müßte gerade sein, entgegen der Kongruenz $v'v \equiv 1$; also ist

$$(10.) \qquad \Sigma v' = \Sigma v.$$

Setzt man nun

$$(11.) \qquad v + v' = 2s,$$

so ist s eine der Zahlen $1, 2, 3, \ldots p-2$; dem Werte $s = 1$ entsprechen $v = v' = 1$. Da aus den Beziehungen

$$(12.) \qquad v + v' = 2s, \quad vv' \equiv 1 \pmod{p}$$

sich v, v' als Wurzeln der Kongruenz

$$z^2 - 2sz + 1 \equiv 0 \pmod{p}$$

ergeben, welche nur für $s = 1$ einander gleich sind, so entsprechen jedem der übrigen zulässigen Werte von s nur zwei Paare von Zahlen: v, v' und v', v; es gibt daher außer $s = 1$ genau $\frac{\alpha-1}{2}$ zulässige Werte

$$(13.) \qquad s_1, s_2, \ldots s_{\frac{\alpha-1}{2}}$$

von s. Addiert man dann alle Gleichungen (11.), so findet sich wegen (10.)

$$(14.) \qquad \Sigma v = 1 + 2s_1 + 2s_2 + \cdots + 2s_{\frac{\alpha-1}{2}}.$$

3. Um die Zahlen (13.) zu bestimmen, verstehe man jetzt unter s eine der Zahlen $2, 3, \ldots p-2$ und bemerke, daß aus den Beziehungen (12.) oder aus den Gleichungen

$$v+v'=2s,\quad vv'=1+2px,$$

worin $x>0$, wenn $s>1$ ist, sich v, v' als die Wurzeln der *Gleichung*

$$z^2-2sz+1+2px=0$$

ergeben, deren Wurzeln

$$z=s\pm\sqrt{s^2-1-2px}$$

sind. Damit die letzteren ganze Zahlen sind, muß der Ausdruck

$$s^2-1-2px$$

das Quadrat einer ganzen Zahl t sein, die positiv gedacht werden darf:

(15.) $$s^2-1-2px=t^2,$$

wodurch $t<s$ folgt; da es mit s von ungleicher Parität ist, werden dann die Wurzeln positiv und ungerade sein; damit sie aber auch kleiner als p ausfallen, muß $s+t<p$ oder $t<p-s$ sein. Diese notwendigen Bedingungen sind offenbar auch dafür hinreichend, daß s eine der Zahlen (13.) sei. Nun erfordert das Bestehen der Gleichung (15.), daß

(16.) $$\left(\frac{t^2+1}{p}\right)=1$$

ist, während wegen $t<s$ und $t<p-s$ auch

(17.) $$0<t<\frac{p}{2}$$

sein muß. Ist t ein diesen Bedingungen gehorchender Wert, so hat die Kongruenz

(18.) $$z^2\equiv t^2+1 \pmod{p}$$

zwei Wurzeln s und $\sigma=p-s$, deren kleinere s sei, so daß $s<\frac{p}{2}$ ist. Eine dieser Wurzeln ist ungleichartig mit t; ist es die Wurzel s, mithin $(-1)^{s+t+1}=1$, so erfüllt die Zahl s die Gleichung (15.) und ist eine Zahl s_i der Reihe (13.), sobald $s>t$ ist; ist es dagegen die Wurzel σ, also

$$(-1)^{p-s+t+1}=1 \text{ oder } (-1)^{s+t+1}=-1,$$

so besteht eine Gleichung

$$\sigma^2-1-2px=t^2,$$

und σ wird gewiß eine Zahl s_i der Reihe (13.) sein, wenn wieder $s>t$ gedacht wird; daher wird dann $-s$ dieser Zahl s_i (mod. p) kongruent sein. Somit ist immer, wenn die kleinere Wurzel s der Kongruenz (18.), d. i. diejenige, welche $<\frac{p}{2}$ ist, größer als t ist,

$$(-1)^{s+t+1}\cdot s$$

einer Zahl s_i der Reihe (13.) kongruent (mod. p). Da aber auf solche

Weise, wenn t alle den Bedingungen (16.) und (17.) gehorchenden Werte durchläuft, sämtliche Zahlen (13.) erhalten werden müssen und jede nur einmal entstehen kann, weil jedem zulässigen Werte von s nach der Gleichung (15.) oder nach der Kongruenz

$$s^2 \equiv t^2 + 1 \pmod{p}$$

nur ein Wert $t < \frac{p}{2}$ entspricht, so findet sich die Kongruenz

$$(19.) \qquad s_1 + s_2 + \cdots + s_{\frac{a-1}{2}} \equiv \Sigma(-1)^{s+t+1} \cdot s \pmod{p},$$

wo die Summation auf alle diejenigen positiven Zahlen $t < \frac{p}{2}$ zu erstrecken ist, für welche $\left(\frac{t^2+1}{p}\right) = 1$ und die kleinere Wurzel s der Kongruenz (18.) größer als t ist.

Bedeutet aber $\sigma = p - s$ die zweite Wurzel dieser Kongruenz, welche nun $< p - t$ ist, so findet sich

$$(-1)^{\sigma+t+1} \cdot \sigma = (-1)^{s+t} \cdot (p - s) \equiv (-1)^{s+t+1} \cdot s \pmod{p},$$

und da zugleich $\operatorname{sgn}(\sigma - t) = \operatorname{sgn}(s - t) = 1$ ist, kommt

$$(20.) \quad 2 \cdot \Sigma(-1)^{s+t+1} s \equiv \Sigma[\operatorname{sgn}(s-t) \cdot (-1)^{s+t+1} \cdot s + \operatorname{sgn}(\sigma - t) \cdot (-1)^{\sigma+t+1} \cdot \sigma],$$

wo die Summation auf diejenigen positiven Zahlen $t < \frac{p}{2}$ zu erstrecken ist, für welche $\left(\frac{t^2+1}{p}\right) = 1$ ist und die beiden Wurzeln s, σ der Kongruenz (18.) zwischen t und $p - t$ liegen. Ist aber für ein der Bedingung $\left(\frac{t^2+1}{p}\right) = 1$ genügendes $t < \frac{p}{2}$ die kleinere Wurzel s der Kongruenz (18.) kleiner als t, so ist ihre größere Wurzel σ größer als $p - t$, und man findet wieder

$$(-1)^{\sigma+t+1} \cdot \sigma \equiv (-1)^{s+t+1} \cdot s \pmod{p},$$

dagegen $\operatorname{sgn}(\sigma - t) = -\operatorname{sgn}(s - t)$, mithin

$$\operatorname{sgn}(\sigma - t) \cdot (-1)^{\sigma+t+1} \cdot \sigma + \operatorname{sgn}(s - t) \cdot (-1)^{s+t+1} \cdot s \equiv 0.$$

Man darf daher jedes Glied dieser Art der Summe zur Rechten von (20.) hinzufügen oder die Summation auf sämtliche $t < \frac{p}{2}$, für welche $\left(\frac{t^2+1}{p}\right) = 1$ ist, erstrecken und unter s, σ die beiden Wurzeln der zugehörigen Kongruenz (18.) verstehen. Diese sind aber zugleich auch die beiden Wurzeln der Kongruenz

$$z^2 \equiv r^2 + 1 \pmod{p},$$

worin $\tau = p - t$ gedacht ist; da nun leicht die Kongruenzen

$$\operatorname{sgn}(s-\tau)\cdot(-1)^{s+\tau+1}\cdot s \equiv \operatorname{sgn}(\sigma-t)\cdot(-1)^{\sigma+t+1}\cdot\sigma,$$
$$\operatorname{sgn}(\sigma-\tau)\cdot(-1)^{\sigma+\tau+1}\cdot\sigma \equiv \operatorname{sgn}(s-t)\cdot(-1)^{s+t+1}\cdot s$$

bestätigt werden, darf die Summation zur Rechten von (20.), statt auf alle t, auch auf alle τ ausgedehnt und die Kongruenz (20.) auch folgendermaßen geschrieben werden:

$$(21.)\qquad 4\cdot\Sigma(-1)^{s+t+1}\cdot s \equiv \Sigma\operatorname{sgn}(s-t)\cdot(-1)^{s+t+1}\cdot s,$$

wenn nunmehr rechts die Summation einfach über alle Lösungen der Kongruenz

$$(22.)\qquad s^2 \equiv t^2+1 \pmod{p}$$

in positiven ganzen Zahlen, welche $<p$ sind, ausgedehnt wird. Mit Rücksicht auf die Formeln (10.), (14.), (19.) und (21.) erhält man daher jetzt *die Kongruenz* (9.) *in nachstehender Gestalt*

$$(23.)\qquad \frac{2^{p-1}-1}{p}+\left(\frac{p-1}{2}\right)^2-2 \equiv \Sigma\operatorname{sgn}(s-t)\cdot(-1)^{s+t+1}\cdot s \pmod{p}.$$

4. Diese Zurückführung der Aufgabe auf eine ganz anders geartete, nämlich auf die Auflösung der Kongruenz (22.), scheint mir nicht ohne Interesse. Durch Einführung eines Multiplikators $w(z)$ aber, welcher gleich 1 ist, wenn z durch p teilbar, gleich 0, wenn z nicht durch p teilbar ist, so daß für jede ganze Zahl $\varkappa$

$$w(\varkappa p+z) = w(z)$$

ist, läßt sich die obige Summe mit Bezug auf s und t unabhängig voneinander auf alle Zahlen von 1 bis $p-1$ ausdehnen und die rechte Seite der Kongruenz (23.) ersetzen durch

$$(24.)\qquad \Sigma\Sigma\operatorname{sgn}(s-t)\cdot(-1)^{s+t+1}\cdot s\cdot w(s^2-t^2-1);$$

man braucht auch diejenigen Kombinationen s, t nicht auszuschließen, bei welchen $s=t$, das Symbol $\operatorname{sgn}(s-t)$ also unbestimmt ist, weil für sie $w(s^2-t^2-1)=0$ ist. Faßt man in der so ausgedehnten Doppelsumme die Glieder zusammen, welche einem bestimmten t entsprechen, so gibt dies den Ausdruck

$$-\sum_{s=1}^{t-1}(-1)^{s+t+1}\cdot s\cdot w(s^2-t^2-1)+\sum_{s=t+1}^{p-1}(-1)^{s+t+1}\cdot s\cdot w(s^2-t^2-1),$$

welcher, wenn im ersten Teile s durch $t-s$, im zweiten durch $t+s$ ersetzt wird, übergeht in

$$\sum_{s=1}^{t-1}(-1)^s\cdot(t-s)w(s^2-2ts-1)-\sum_{s=1}^{p-t-1}(-1)^s\cdot(t+s)w(s^2+2ts-1),$$

oder endlich, wenn hier im zweiten Teile $p-s$ für s gesetzt wird, und Vielfache von p vernachlässigt werden, in

$$\sum_{s=1}^{p-1}(-1)^s(t-s)\cdot w(s^2-2ts-1).$$

Demnach wird die Doppelsumme in (23.) zunächst kongruent mit

$$\sum_{s=1}^{p-1}\sum_{t=1}^{p-1}(-1)^s(t-s)\cdot w(s^2-2ts-1) \pmod{p}$$

oder, da für jedes s aus der Reihe $2, 3, \ldots p-2$ ein einziges t der Reihe $1, 2, 3, \ldots p-1$ vorhanden ist, für welches $s^2-2ts-1\equiv 0 \pmod{p}$ wird, für $s=1$ und $s=p-1$ aber $w(s^2-2ts-1)=0$ ist, kongruent mit

$$\sum_{s=1}^{p-1}\sum_{t=1}^{p-1}(-1)^s t\cdot w(s^2-2ts-1)-\sum_{s=2}^{p-2}(-1)^s\cdot s,$$

d. h. mit

$$\sum_{s=1}^{p-1}\sum_{t=1}^{p-1}(-1)^s t\cdot w(s^2-2ts-1)-\frac{p-1}{2}-2 \pmod{p}.$$

Die Kongruenz (23.) *erhält hierdurch die neue Gestalt:*

$$(25.)\quad \frac{2^{p-1}-1}{p}+\frac{p^2-1}{4}\equiv\sum_{s=1}^{p-1}\sum_{t=1}^{p-1}(-1)^s t\cdot w(s^2-2ts-1) \pmod{p}.$$

5. Man darf, unter r die primitive p-te Einheitswurzel

$$r=e^{\frac{2\pi i}{p}}$$

verstehend,

$$w(z)=\frac{1}{p}\cdot\sum_{h=0}^{p-1}r^{hz}$$

wählen. Dann verwandelt sich die in der letzten Kongruenz auftretende Doppelsumme in eine dreifache, deren Summationen wir anordnen, wie folgt:

$$(26.)\qquad \frac{1}{p}\cdot\sum_{s=1}^{p-1}(-1)^s\cdot\sum_{h=0}^{p-1}r^{(s^2-1)h}\sum_{t=1}^{p-1}t\cdot r^{-2sht}.$$

Nun ist für jede primitive p-te Einheitswurzel ϱ

$$0=1+\varrho+\varrho^2+\cdots+\varrho^{p-2}+\varrho^{p-1}.$$

Setzt man also

$$R=1\cdot\varrho+2\cdot\varrho^2+3\cdot\varrho^3+\cdots+(p-1)\cdot\varrho^{p-1}$$

und addiert diese Gleichung zur vorhergehenden, so erhält man die Beziehung

$$R=1+2\varrho+3\varrho^2+4\varrho^3+\cdots+(p-1)\varrho^{p-2}+p\varrho^{p-1},$$

d. i.

$$R=\varrho^{p-1}\cdot R+p\varrho^{p-1},$$

mithin

$$R = -\frac{\varrho^{p-1}}{\varrho^{p-1}-1}\cdot p = -\frac{\varrho^{\frac{p-1}{2}}}{\varrho^{\frac{p-1}{2}}-\varrho^{-\frac{p-1}{2}}}\cdot p.$$

Indem man für $h>0$ hier $\varrho = r^{-2sh}$ wählt und den sich für R ergebenden Wert in (26.) einsetzt, geht die dreifache Summe über in die zweifache:

$$\sum_{s=1}^{p-1}(-1)^{s+1}\cdot\left[\sum_{h=1}^{p-1}\frac{r^{(s^2+s-1)h}}{r^{sh}-r^{-sh}} - \frac{p-1}{2}\right],$$

die jedoch einfacher geschrieben werden kann, wie folgt:

$$(27.)\qquad \sum_{s=1}^{p-1}(-1)^{s+1}\cdot\sum_{h=1}^{p-1}\frac{r^{(s^2+s-1)h}}{r^{sh}-r^{-sh}}.$$

Bei Umkehrung der Summationsordnung, und wenn dann bei der Summation nach s die geraden Werte g und die ungeraden Werte u von s unterschieden und die letzteren durch $p-g$ ersetzt werden, nimmt die Doppelsumme folgende Gestalt an:

$$-\sum_{h=1}^{p-1} r^{-h}\cdot\sum_{g}\frac{r^{g/2\cdot 2gh}+r^{(g/2+1)\cdot 2gh}}{r^{2gh}-1}$$

$$= -\sum_{h=1}^{p-1} r^{-h}\sum_{g}\left(r^{g/2\cdot 2gh}+2\cdot r^{(g/2-1)2gh}+\cdots+2r^{2gh}+2\right) - 2\cdot\sum_{h=1}^{p-1} r^{-h}\sum_{g}\frac{1}{r^{2gh}-1}.$$

Wenn nun aber bei der ersten dieser beiden Doppelsummen wieder zuerst nach h summiert wird, so findet sie sich leicht kongruent mit

$$-\sum_{g}(g+1) \equiv -\frac{p^2-1}{4} - \frac{p-1}{2}.$$

Der Ausdruck (27.) wird daher kongruent mit

$$\frac{p^2-1}{4}+\frac{p-1}{2} - 2\cdot\sum_{h=1}^{p-1} r^{-h}\sum_{g}\frac{1}{r^{2gh}-1}.$$

Da das allgemeine Glied der letzten Doppelsumme bei Vertauschung von h mit $p-h$ in

$$r^h\cdot\frac{1}{r^{-2gh}-1} = -r^h - r^h\cdot\frac{1}{r^{2gh}-1}$$

übergeht, so darf man die zweifach genommene Doppelsumme auch durch

$$\frac{p-1}{2} - \sum_{h=1}^{p-1}(r^h - r^{-h})\cdot\sum_{g}\frac{1}{r^{2gh}-1}$$

ersetzen. *Hiernach gewinnt man aus der Kongruenz* (25.) *die nachstehende:*

$$(28.)\qquad \frac{2^{p-1}-1}{p} \equiv \sum_{h=1}^{p-1}(r^h - r^{-h})\sum_{g}\frac{1}{r^{2gh}-1},$$

der man, wenn

$$(29.) \qquad f_h(x) = \prod_g (x - r^{2gh}) = \prod_{s=1}^{\frac{p-1}{2}} (x - r^{4hs})$$

gesetzt wird, die Gestalt geben kann:

$$(30.) \qquad \frac{2^{p-1}-1}{p} \equiv \sum_{h=1}^{p-1} (r^{-h} - r^h) \cdot \frac{f_h'(1)}{f_h(1)} \pmod{p}.$$

Der Ausdruck

$$f_{-h}(x) = \prod_g (x - r^{-2gh}) = \prod_{s=1}^{\frac{p-1}{2}} (x - r^{-4hs})$$

ist konjugiert imaginär zu $f_h(x)$ und

$$f_h(x) \cdot f_{-h}(x) = F(x) = \frac{x^p - 1}{x - 1},$$

mithin

$$\frac{f_h'(x)}{f_h(x)} + \frac{f_{-h}'(x)}{f_{-h}(x)} = \frac{F'(x)}{F(x)},$$

und insbesondere für $x = 1$

$$\frac{f_h'(1)}{f_h(1)} + \frac{f_{-h}'(1)}{f_{-h}(1)} = \frac{F'(1)}{F(1)} = \frac{p-1}{2};$$

daher ist der reelle Bestandteil von $\frac{f_h'(1)}{f_h(1)}$ gleich $\frac{p-1}{4}$. Von diesem darf aber in der Formel (30.) abgesehen werden, da offenbar

$$\sum_{h=1}^{p-1} (r^{-h} - r^h) \cdot \frac{p-1}{4} = 0$$

ist. *Nennt man also* I_h *den imaginären Bestandteil von* $\frac{f_h'(1)}{f_h(1)}$, *so gilt die Kongruenz:*

$$(31.) \qquad \frac{2^{p-1}-1}{p} \equiv \sum_{h=1}^{p-1} (r^{-h} - r^h) \cdot I_h \pmod{p}.$$

Die Formel (28.), der wir diese letzte Gestalt gegeben haben, läßt sich direkter wiedergewinnen. Ich habe hier den Weg mitgeteilt, auf dem ich sie zuerst gefunden, weil ich glaubte, die Formel (23.), aus der sie fließt, nicht unterdrücken zu sollen. Bisher gelang es mir nun noch nicht, für I_h einen einfachen Ausdruck zu finden, der geeignet wäre, weitere Schlüsse über den Rest von $\frac{2^{p-1}-1}{p}$ (mod. p) zu ziehen; doch scheint mir die Zurückführung dieser Frage auf ein Gebiet der Kreisteilung, welchem die *Gauß*schen Summen angehören, wertvoll genug, um eine Mitteilung davon zu rechtfertigen.