Zur Theorie der quadratischen Reste.

(Von Herrn *Stern* zu Göttingen.)

1. In dem ersten Hefte dieses Bandes des Journals habe ich die Frage behandelt, wenn man die Zahlen $1, 2, \ldots \frac{1}{2}(p-1)$ auf alle möglichen Weisen mit $+$ und $-$ verbindet, während p eine Primzahl ist, wie viele dieser Aggregate, nach dem Modul p, einem quadratischen Reste oder Nichtreste oder Null congruent sind. Eine ähnliche Frage ist folgende. Wenn man die sämmtlichen quadratischen Reste einer Primzahl p auf alle möglichen Weisen mit $+$ oder $-$ verbindet, wie viele dieser Aggregate werden einem quadratischen Reste oder einem quadratischen Nichtreste oder Null congruent sein? Die Zahl $p = 3$ bleibt hierbei, da sie nur einen einzigen quadratischen Rest hat, von selbst ausgeschlossen.

Da im Folgenden nur von *quadratischen* Resten die Rede ist, so werde ich diese, der Kürze halber, nur *Reste* nennen, sowie die *quadratischen* Nichtreste nur *Nichtreste*. Die einzelnen Reste sollen durch $a_1, a_2, \ldots a_{\frac{1}{2}(p-1)}$ bezeichnet werden und irgend einer derselben durch a; ebenso die einzelnen Nichtreste durch $b_1, b_2, \ldots b_{\frac{1}{2}(p-1)}$ und irgend einer derselben durch b. Ferner soll r eine Wurzel der Gleichung $x^p-1=0$ bedeuten (die Einheit ausgenommen) und zwar wählen wir dafür den einfachsten Werth, also

$$r = \cos\frac{2\pi}{p} + \sin\frac{2\pi}{p}\cdot i.$$

Diesem entsprechend sei

$$\Pi(1+r^a) = (1+r^{a_1})(1+r^{a_2})\ldots(1+r^{a_{\frac{1}{2}(p-1)}}),$$

woraus sich von selbst die Bedeutung von $\Pi(1+r^b)$, $\Pi(1-r^a)$, $\Pi(1-r^b)$, u. s. w. ergiebt.

2. Die oben angedeutete Frage lässt sich auf eine andere zurückführen. Addirt man nemlich die sämmtlichen Reste der Zahl p in der Weise, dass man k derselben mit dem $+$ Zeichen, die übrigen mit dem $-$ Zeichen nimmt, so ist dieses Aggregat, nach dem Modul p, der Zahl congruent, die man erhält, wenn man nur die k positiven Reste addirt und die Summe mit 2 multiplicirt. Bezeichnet man nemlich diese Summe durch S, die Summe der negativen Reste durch $-s$, so hat man $S-s = 2S-(S+s)$. Nun ist

$S+s \equiv 0$, also $S-s \equiv 2S$. Statt die Zahlen zu suchen, welchen die aus sämmtlichen Resten, von denen k positiv, die übrigen negativ sind, gebildeten Aggregate congruent sind, hat man daher nur die Zahlen zu suchen, welchen die Combinationen*) der k^{ten} Classe, gebildet aus den mit 2 multiplicirten Resten, congruent sind, indem man die in jeder Combination enthaltenen Elemente mit + verbindet. Und demnach kann man, statt der im vorigen §. angegebenen Frage, folgende stellen: Man multiplicirt die einzelnen Reste mit 2 und bildet aus den so erhaltenen Zahlen als Elementen sämmtliche Combinationen aus allen Classen, indem man die in jeder Combination enthaltenen Zahlen mit + verbindet. Wie viele dieser Combinationen werden einem Reste oder Nichtreste oder Null congruent sein?

Es wird hierbei nur zu beachten sein, dass einem der Aggregate aus sämmtlichen Resten keine Combination entspricht, demjenigen nemlich, bei welchem sämmtliche Reste das − Zeichen haben. Da aber dieses Aggregat $\equiv 0$ ist, so wird man nur die Anzahl der Combinationen die $\equiv 0$ sind, um eine Einheit zu vermehren haben, wenn man die Anzahl der Aggregate, die $\equiv 0$ sind, finden will.

Es wird aber offenbar genügen, die Combinationen aus den einfachen Resten, statt aus dem Doppelten derselben, zu bilden. Denn, wenn 2 ein Rest ist, so hat man in beiden Fällen dieselben Elemente; ist dagegen 2 ein Nichtrest, so entspricht jedem Reste a oder Nichtreste b, welchem eine aus den Resten gebildete Combination congruent ist, ein Nichtrest $2a$ oder Rest $2b$, welchem die aus dem Doppelten dieser Reste gebildete Combination congruent ist.

Giebt es m Combinationen aus den Resten, welche einer Zahl k congruent sind, so sage ich: die Zahl k kommt m mal unter den Combinationen vor. Es ist also die Frage zu beantworten, wie oft jede Zahl, Null eingeschlossen, unter den Combinationen aus den Resten vorkommt.

3. Man setze

$$(1.) \qquad \Pi(1+r^a) = (1+r)(1+r^4)\ldots\left(1+r^{\left(\frac{p-1}{2}\right)^2}\right) = 1+A_1 r+A_2 r^2+\ldots+A_p r^p.$$

Die Zahlen A_1, A_2, ... A_p geben also an, wie oft die Zahlen 1, 2, ... 0 unter den Combinationen aus den Resten vorkommen. Nun ist zunächst leicht zu sehen, dass unter diesen Combinationen alle Reste gleich oft und auch

*) Unter Combinationen werden im Folgenden immer Combinationen ohne Wiederholung verstanden.

alle Nichtreste gleich oft vorkommen. Man kann sogar noch allgemeiner beweisen, dass dies bei jeder einzelnen Combinationsclasse der Fall sein muss. Ist die in der k^{ten} Classe vorkommende Combination $a_1+a_2+\cdots+a_k$ einem Reste congruent, so dass man $a_1+a_2+\cdots+a_k \equiv a$ hat, und multiplicirt man diese Congruenz mit allen einzelnen Resten, so erhält man $\frac{1}{2}(p-1)$ Congruenzen, die ebenso viel Combinationen der k^{ten} Classe repräsentiren, von denen jede einem anderen Reste congruent ist. Sobald also unter den Combinationen der k^{ten} Classe *ein* Rest vorkommt, müssen *alle* Reste darunter vorkommen. Zugleich müssen alle diese Reste gleich oft vorkommen. Käme nemlich der Rest a_r unter den Combinationen m mal vor, der Rest a_s aber nicht so oft, so dass man also m Congruenzen von der Form $a_1+a_2+\cdots+a_k \equiv a_r$ hätte, so liesse sich jedenfalls ein Rest a_t finden, welcher der Congruenz $a_r a_t \equiv a_s$ genügte. Indem man also jene m Congruenzen mit a_t multiplicirte, erhielte man m Congruenzen, welche ebenso viel Combinationen der k^{ten} Classe aus den Resten repräsentiren, die congruent a_s wären, gegen die Voraussetzung. Man beweist ebenso, dass auch alle Nichtreste in gleicher Zahl in jeder Combinationsclasse vorkommen. Es folgt ferner, dass auch bei den Combinationen aus den Nichtresten in jeder Combinationsclasse alle Reste gleich oft und alle Nichtreste gleich oft vorkommen müssen. Zugleich ist klar, dass, wenn unter den Combinationen irgend einer Classe aus den Resten jeder Rest m mal und jeder Nichtrest n mal vorkommt, unter den Combinationen derselben Classe aus den Nichtresten jeder Rest n mal und jeder Nichtrest m mal vorkommen muss. Denn aus jeder Combination der Reste, welche einem Reste oder einem Nichtreste congruent ist, ergiebt sich, wenn man die einzelnen Elemente dieser Combination mit einem Nichtreste multiplicirt, eine Combination derselben Classe aus den Nichtresten, die einem Nichtreste oder Reste congruent ist. Die Null muss dagegen unter den Combinationen aus den Resten ebenso oft vorkommen, als unter den Combinationen aus den Nichtresten.

4. Setzt man

$$\Sigma r^a = r^{a_1}+r^{a_2}+\cdots+r^{a_{\frac{1}{2}(p-1)}},$$

$$\Sigma r^b = r^{b_1}+r^{b_2}+\cdots+r^{b_{\frac{1}{2}(p-1)}},$$

$$l = 1+A_p$$

und nimmt man an, dass die Reste m mal, die Nichtreste n mal unter den Combinationen aus den Resten vorkommen, so kann man statt der Gleichung (1.)

auch schreiben:

$$(2.) \qquad \Pi(1+r^a) = l + m\Sigma r^a + n\Sigma r^b,$$

woraus

$$\Pi(1+r^b) = l + n\Sigma r^a + m\Sigma r^b$$

folgt. Aus

$$\Pi(1-r^a) = \Pi\left(1-\cos\frac{2a\pi}{p} - \sin\frac{2a\pi}{p}\,i\right)$$

folgt, wegen $\sin\frac{2a\pi}{p} = 2\sin\frac{a\pi}{p}\cos\frac{a\pi}{p}$ und $1-\cos\frac{2a\pi}{p} = 2\left(\sin\frac{a\pi}{p}\right)^2$

$$\Pi(1-r^a) = (-1)^{\frac{1}{2}(p-1)}(2i)^{\frac{1}{2}(p-1)}\Pi\sin\frac{a\pi}{p}\cdot e^{\Sigma a\cdot\frac{\pi}{p}i},$$

wo e die Basis der natürlichen Logarithmen und Σa die Summe der Reste bezeichnet. Da nun $e^{\pi i} = -1$, und Σa und $\frac{\Sigma a}{p}$ zugleich gerade oder ungerade sind, so hat man auch

$$(3.) \qquad \Pi(1-r^a) = (-1)^{\frac{1}{2}(p-1)}(2i)^{\frac{1}{2}(p-1)}\Pi\sin\frac{a\pi}{p}(-1)^{\Sigma a}$$

und ebenso findet man

$$\Pi(1-r^b) = (-1)^{\frac{1}{2}(p-1)}(2i)^{\frac{1}{2}(p-1)}\Pi\sin\frac{b\pi}{p}(-1)^{\Sigma b}.$$

5. Sei nun $p = 4\nu+3$, dann entspricht jedem Reste a ein Nichtrest $p-a$, man hat daher $\Pi\sin\frac{a\pi}{p} = \Pi\sin\frac{b\pi}{p}$ und

$$\frac{\Pi(1-r^a)}{\Pi(1-r^b)} = (-1)^{\Sigma a-\Sigma b}.$$

Nun ist $\Sigma a+\Sigma b = \frac{p(p-1)}{2}$ eine ungerade Zahl, von den zwei Zahlen Σa, Σb ist also immer die eine gerade, die andere ungerade, folglich

$$(4.) \qquad \frac{\Pi(1-r^a)}{\Pi(1-r^b)} = -1.$$

Ist nun $p = 8k+7$, also 2 ein Rest, so ist

$$\Pi(1+r^a)\Pi(1-r^a) = \Pi(1-r^{2a}) = \Pi(1-r^a),$$
$$\Pi(1+r^b)\Pi(1-r^b) = \Pi(1-r^{2b}) = \Pi(1-r^b),$$

d. h.

$$(5.) \qquad \Pi(1+r^a) = 1, \qquad \Pi(1+r^b) = 1.$$

Ist $p = 8k+3$, also 2 ein Nichtrest, so ist

$$\Pi(1+r^a)\Pi(1-r^a) = \Pi(1-r^b),$$

mithin nach (4.)

$$(6.) \qquad \Pi(1+r^a)=-1, \qquad \Pi(1+r^b)=-1.$$

Für die Zahlen $p=8k+7$ folgt mithin aus (2.)

$$A_p+m\Sigma r^a+n\Sigma r^b = 0,$$

welcher Gleichung nur Genüge geleistet werden kann, wenn

$$A_p=m=n.$$

Nun ist die Anzahl aller Combinationen aus den $\frac{1}{2}(p-1)$ Resten

$$A_p+(m+n)\left(\frac{p-1}{2}\right),$$

also nach dem Vorhergehenden gleich pA_p, andererseits ist diese Anzahl $=2^{\frac{1}{2}(p-1)}-1$, mithin

$$A_p=m=n=\frac{2^{\frac{1}{2}(p-1)}-1}{p}=A_1=A_2=\cdots=A_{p-1}.$$

Ist dagegen $p=8k+3$, so hat man nach (6.)

$$l+m\Sigma r^a+n\Sigma r^b = -1,$$

oder

$$2+A_p+m\Sigma r^a+n\Sigma r^b = 0.$$

Damit diese Gleichung bestehen kann, muss also

$$2+A_p=m=n$$

sein. Man hat mithin

$$A_p+2(2+A_p)\left(\frac{p-1}{2}\right) = 2^{\frac{1}{2}(p-1)}-1,$$

d. h.

$$A_p = \frac{2^{\frac{1}{2}(p-1)}+1}{p}-2,$$

$$m=n=\frac{2^{\frac{1}{2}(p-1)}+1}{p}=A_1=A_2=\cdots=A_{p-1}.$$

Hieraus folgt demnach der Satz:

Bildet man aus den Resten einer Primzahl $p=4\nu+3$ sämmtliche Combinationen, so kommen unter diesen alle Reste und alle Nichtreste gleich oft vor und zwar jeder $\frac{2^{\frac{1}{2}(p-1)}\pm 1}{p}$ mal, wo das obere oder untere Zeichen zu nehmen ist, je nachdem $p=8k+3$ oder $8k+7$ ist. Die Null kommt im ersten Falle $\frac{2^{\frac{1}{2}(p-1)}+1}{p}-2$ mal, im zweiten $\frac{2^{\frac{1}{2}(p-1)}-1}{p}$ mal vor.

Uebrigens ergiebt sich aus dem Vorhergehenden von selbst, dass dasselbe Verhältniss auch bei den Combinationen aus den Nichtresten stattfindet.

6. Setzt man noch immer voraus, dass $p = 4\nu+3$, so hat man

$$\Pi(1-r^a) = (1-r)(1-r^4)\dots\left(1-r^{\left(\frac{p-1}{2}\right)^2}\right),$$

$$\Pi(1-r^b) = (1-r^{-1})(1-r^{-4})\dots\left(1-r^{-\left(\frac{p-1}{2}\right)^2}\right),$$

und, wie bekannt,

$$(7.) \qquad \Pi(1-r^a)\Pi(1-r^b) = p.$$

Nun setze man

$$(8.) \qquad \Pi(1-r^a) = \beta_0+\beta_1 r \ +\beta_2 r^2 \ +\dots+\beta_{p-1}r^{p-1},$$

also

$$(8'.) \qquad \Pi(1-r^b) = \beta_0+\beta_1 r^{-1}+\beta_2 r^{-2}+\dots+\beta_{p-1}r^{-(p-1)}.$$

Hier bezeichnet β_h, wenn nicht $h=0$ ist, wie oft die Zahl h in den geraden Classen der aus den Resten gebildeten Combinationen mehr vorkommt als in den ungeraden, dagegen ist $\beta_0 = 1+\beta_p$, wo β_p andeutet, wie oft Null in den geraden Classen mehr vorkommt als in den ungeraden.

Aus den Gleichungen (7.) und (8.) ergiebt sich sofort, wie ich schon bei einem ähnlichen Fall in meinem früheren Aufsatze §. 5 gezeigt habe,

$$(9.) \qquad \beta_0^2+\beta_1^2+\dots+\beta_{p-1}^2 = p-1,$$

$$(10.) \qquad \beta_0+\beta_1+\dots+\beta_{p-1} = 0.$$

Da aber $A_k = \dfrac{2^{\frac{1}{2}(p-1)}\pm 1}{p}$, also eine ungerade Zahl ist, wenn k eine der Zahlen $1, 2, \dots p-1$ ist, so kann keine der Zahlen $\beta_1^2, \beta_2^2, \dots \beta_{p-1}^2$ Null sein. Damit die Gleichung (9.) bestehen kann, muss also $\beta_0=0$, d. h. $\beta_p=-1$ sein, woraus mithin folgt, dass die Null in den geraden Classen einmal weniger vorkommt als in den ungeraden. Es folgt ferner, dass jede der Zahlen $\beta_1, \beta_2, \dots \beta_{p-1}$ der positiven oder negativen Einheit gleich ist, und zwar muss nach (10.) die Hälfte dieser Zahlen positiv und die andere Hälfte negativ sein. Es kommt also nur noch darauf an, das Zeichen allgemein zu bestimmen.

Aus der bekannten Gleichung

$$\sin\frac{\pi}{p}\sin\frac{2\pi}{p}\sin\frac{3\pi}{p}\cdots\sin\frac{p-1}{p}\pi = \frac{p}{2^{p-1}}$$

folgt, da $p = 4\nu+3$,

$$\left[\Pi\sin\frac{a\pi}{p}\right]^2 = \frac{p}{2^{p-1}}$$

und, da $\Pi \sin \frac{a\pi}{p}$ positiv ist,

$$\Pi \sin \frac{a\pi}{p} = \frac{\sqrt{p}}{2^{\frac{1}{2}(p-1)}}.$$

Mithin nach Gleichung (3.)

$$\Pi(1-r^a) = (-i)^{\frac{1}{2}(p-1)} \sqrt{p}\,(-1)^{\Sigma a}.$$

Ferner ist

$$\Sigma r^a - \Sigma r^b = r - r^{-1} + r^4 - r^{-4} + \cdots + r^{\left(\frac{p-1}{2}\right)^2} - r^{-\left(\frac{p-1}{2}\right)^2} = i\,\Sigma 2 \sin \frac{2a\pi}{p},$$

aber, wie bekannt,

$$\Sigma 2 \sin \frac{2a\pi}{p} = \sqrt{p},$$

also

$$\Sigma r^a - \Sigma r^b = i\sqrt{p}$$

und

$$\Pi(1-r^a) = (-1)^{\frac{1}{2}(p-1)} (i)^{\frac{1}{2}(p-3)} [\Sigma r^a - \Sigma r^b] (-1)^{\Sigma a}$$

oder

$$(11.) \qquad \Pi(1-r^a) = \pm [\Sigma r^a - \Sigma r^b] (-1)^{\Sigma a},$$

wo das obere oder untere Zeichen zu nehmen ist, je nachdem $p = 8k+7$ oder $= 8k+3$ ist.

Vergleicht man daher diese Formel mit der Formel (8.), so ergiebt sich, dass für $p = 8k+7$ der Werth von β_h entweder $(-1)^{\Sigma a}$ oder $-(-1)^{\Sigma a}$ ist, je nachdem h ein Rest oder Nichtrest von p ist; bei den Zahlen von der Form $8k+3$ ist es umgekehrt.

Man hat demnach den Satz:

Wenn man aus den Resten alle Combinationen bildet, so ist, wenn $p = 8k+7$, der Unterschied der Zahlen, welche angeben wie oft eine Zahl h in den geraden und in den ungeraden Combinationsclassen vorkommt, $(-1)^{\Sigma a}$ oder $-(-1)^{\Sigma a}$, je nachdem h ein Rest oder Nichtrest ist; bei den Zahlen $p = 8k+3$ ist es umgekehrt.

Da, wie oben bemerkt wurde, von den Zahlen Σa, Σb immer die eine gerade, die andere ungerade ist, so kann man statt $-(-1)^{\Sigma a}$ auch $(-1)^{\Sigma b}$ setzen. Bedenkt man ferner, dass 2 ein Rest oder ein Nichtrest ist, je nachdem $p = 8k+7$ oder $8k+3$, so sieht man, dass man statt der Formel (11.) auch schreiben kann:

$$(12.) \qquad \Pi(1-r^a) = [\Sigma r^a - \Sigma r^b] (-1)^{\Sigma 2a},$$

wenn man unter $\Sigma 2a$ die Summe der Zahlen versteht, die man aus den

Zahlen $2a_1, 2a_2 \ldots 2a_{p-1}$ erhält, wenn man von jeder der letzteren die darin enthaltenen Vielfachen von p abzieht. Man kann demnach den obigen Satz auch so aussprechen:

Der Unterschied der Zahlen, welche angeben, wie oft eine Zahl h in den geraden und in den ungeraden Classen der aus den Resten gebildeten Combinationen vorkommt, ist $(-1)^{\Sigma 2a}$ oder $-(-1)^{\Sigma 2a}$, je nachdem h ein Rest oder Nichtrest ist.

Bedient man sich des bekannten Symbols $\left(\frac{h}{p}\right)$, um die positive oder negative Einheit auszudrücken, je nachdem h ein Rest oder Nichtrest von p ist, so ist mithin dieser Unterschied $\left(\frac{h}{p}\right)(-1)^{\Sigma 2a}$. Zugleich folgt alsdann aus §. 5, dass die Zahl h in jedem Falle $\frac{2^{\frac{1}{2}(p-1)} - \left(\frac{2}{p}\right)}{p}$ mal unter den Combinationen vorkommt. Sobald also h nicht Null ist, kommt diese Zahl in den *geraden* Combinationsclassen $\frac{2^{\frac{1}{2}(p-1)} - \left(\frac{2}{p}\right)}{2p} + \frac{1}{2}\left(\frac{h}{p}\right)(-1)^{\Sigma 2a}$ und in den *ungeraden* $\frac{2^{\frac{1}{2}(p-1)} - \left(\frac{2}{p}\right)}{2p} - \frac{1}{2}\left(\frac{h}{p}\right)(-1)^{\Sigma 2a}$ mal vor.

Ferner folgt aus §. 5, dass die Null $\frac{2^{\frac{1}{2}(p-1)} - \left(\frac{2}{p}\right)}{p} - \left(1 - \left(\frac{2}{p}\right)\right)$ mal unter den Combinationen vorkommt. Da sie nun, wie oben gezeigt wurde, in den geraden Classen einmal weniger als in den ungeraden vorkommt, so ist sie in den ungeraden Classen $\frac{2^{\frac{1}{2}(p-1)} - \left(\frac{2}{p}\right)}{2p} + \frac{1}{2}\left(\frac{2}{p}\right)$ mal enthalten.

Aus der Formel (8′.) ergiebt sich, dass bei den aus den Nichtresten gebildeten Combinationen der Unterschied der Zahlen, welche angeben, wie oft eine Zahl h in den geraden und in den ungeraden Combinationsclassen vorkommt, $(-1)^{\Sigma 2a}$ oder $-(-1)^{\Sigma 2a}$ ist, je nachdem h ein Nichtrest oder Rest ist, also jedenfalls $-\left(\frac{h}{p}\right)(-1)^{\Sigma 2a}$, woraus sich, in Verbindung mit §. 5, ergiebt, dass jede solche Zahl in den geraden Combinationsclassen $\frac{2^{\frac{1}{2}(p-1)} - \left(\frac{2}{p}\right)}{2p} - \frac{1}{2}\left(\frac{h}{p}\right)(-1)^{\Sigma 2a}$ und in den ungeraden $\frac{2^{\frac{1}{2}(p-1)} - \left(\frac{2}{p}\right)}{2p} + \frac{1}{2}\left(\frac{h}{p}\right)(-1)^{\Sigma 2a}$ mal vorkommt. Für $h = 0$ bleiben die früheren Formeln.

7. Sei nun $p = 4\nu+1$. Man setze wieder

$$\Pi(1+r^a) = l+m\Sigma r^a+n\Sigma r^b,$$
$$\Pi(1+r^b) = l+n\Sigma r^a+m\Sigma r^b.$$

Nach dem bekannten *Gauss*schen Satze ist aber in diesem Falle

$$\Sigma r^a = \Sigma\cos\frac{2a\pi}{p} = -\tfrac{1}{2}+\tfrac{1}{2}\sqrt{p}; \qquad \Sigma r^b = \Sigma\cos\frac{2b\pi}{p} = -\tfrac{1}{2}-\tfrac{1}{2}\sqrt{p},$$

also

$$\Pi(1+r^a) = l-\frac{m+n}{2}+\frac{m-n}{2}\sqrt{p},$$
$$\Pi(1+r^b) = l-\frac{m+n}{2}-\frac{m-n}{2}\sqrt{p}.$$

Nun sind die Zahlen l, m, n wieder zunächst durch die Gleichung (§. 5)

$$(13.) \qquad l+(m+n)\frac{p-1}{2} = 2^{\frac{1}{2}(p-1)}$$

verbunden. Ist $p = 8k+1$, also 2 ein Rest, so ist mithin

$$\Pi(1+r^a)\Pi(1-r^a) = \Pi(1-r^a), \quad \Pi(1+r^b)\Pi(1-r^b) = \Pi(1-r^b),$$

d. h.

$$(14.) \qquad \Pi(1+r^a) = 1, \qquad \Pi(1+r^b) = 1,$$

und hieraus folgt wieder $l-1 = A_p = m = n$, also, wegen Formel (13.),

$$(15.) \qquad A_p = m = n = \frac{2^{\frac{1}{2}(p-1)}-1}{p}.$$

Bei den Zahlen von der Form $8k+1$ kommt mithin, wie bei den Zahlen von der Form $8k+7$, unter den Combinationen aus den Resten (sowie auch aus den Nichtresten) jeder Rest und jeder Nichtrest, sowie auch Null, $\frac{2^{\frac{1}{2}(p-1)}-1}{p}$ mal vor.

Bei den Zahlen von der Form $8k+5$ fällt das Resultat weniger einfach aus, wozu folgende Betrachtungen führen.

8. Ist $\frac{x^p-1}{x-1} = X$, so hat man, wie bekannt, $Y^2-pZ^2 = 4X$, wo $Y+Z\sqrt{p} = 2\Pi(x-r^a)$, $Y-Z\sqrt{p} = 2\Pi(x-r^b)$ und Y und Z nach ganzen positiven Potenzen von x geordnete und mit ganzzahligen Coefficienten versehene Reihen sind. Setzt man $x = -1$ und bezeichnet die Werthe, welche dann Y und Z annehmen, durch Y_0 und Z_0, so folgt

$$(16.) \qquad Y_0+Z_0\sqrt{p} = 2\Pi(1+r^a); \qquad Y_0-Z_0\sqrt{p} = 2\Pi(1+r^b).$$

Aus

$$(1+r^a) = 1+\cos\frac{2a\pi}{p}+\sin\frac{2a\pi}{p}i = 2\cos\frac{a\pi}{p}e^{\frac{a\pi}{p}i}$$

folgt, wie in §. 4,

$$\Pi(1+r^a) = 2^{\frac{1}{2}(p-1)}\Pi\cos\frac{a\pi}{p}(-1)^{\Sigma a}.$$

Da nun $p=4\nu+1$, so ist $\Sigma a=\nu p$ und mithin

$$\Pi(1+r^a) = 2^{\frac{1}{2}(p-1)}\Pi\cos\frac{a\pi}{p}(-1)^{\nu}.$$

In dem Producte $\Pi\cos\frac{a\pi}{p}$ ist aber die Anzahl der negativen Factoren gerade oder ungerade, je nachdem ν eine gerade oder ungerade Zahl ist; demnach ist $\Pi(1+r^a)$ jedenfalls positiv, und bezeichnet man den absoluten Werth von $\Pi\cos\frac{a\pi}{p}$ durch W, so hat man

$$\Pi(1+r^a) = 2^{\frac{1}{2}(p-1)}W.$$

Auch ist $\Pi(1+r^a)\Pi(1+r^b)=1$, also

$$\Pi(1+r^b) = \frac{1}{2^{\frac{1}{2}(p-1)}W}.$$

Demnach ist

$$Y_0+Z_0\sqrt{p}=2^{\frac{1}{2}(p+1)}W; \qquad Y_0-Z_0\sqrt{p}=\frac{1}{2^{\frac{1}{2}(p-3)}W}.$$

Es sind also Y_0 und Z_0 ganze Zahlen, die durch Kreisfunctionen bestimmt sind (oder Null). Man bezeichne durch y_0 und z_0 die absoluten Werthe von Y_0 und Z_0. Nun zeigen die vorstehenden Gleichungen, dass jedenfalls Y_0 positiv ist, also $Y_0=y_0$.

Ist $p=8k+1$, so folgt aus (14.) und (16.)

$$Y_0=y_0=2, \qquad Z_0=z_0=0.$$

9. Bezeichnet man durch Y' und Z' das, was aus Y und Z wird, wenn man $x=1$ setzt, so folgt aus den obigen Gleichungen

$$Y'+Z'\sqrt{p} = 2\Pi(1-r^a),$$
$$Y'-Z'\sqrt{p} = 2\Pi(1-r^b).$$

Aus Formel (3.) folgt aber, da $p=4\nu+1$,

$$\Pi(1-r^a)=2^{\frac{1}{2}(p-1)}\Pi\sin\frac{a\pi}{p}; \qquad \Pi(1-r^b)=2^{\frac{1}{2}(p-1)}\Pi\frac{\sin b\pi}{p},$$

so dass Y' und Z' ebenfalls durch Kreisfunctionen bestimmt sind. Nun hat schon *Dirichlet* gezeigt (Bd. 18 dieses Journals p. 270), dass Y' positiv, Z' negativ ist. Bezeichnet man also die absoluten Werthe von Y' und Z' durch y' und z', so hat man

$$(17.) \qquad y'-z'\sqrt{p}=2\Pi(1-r^a), \qquad y'+z'\sqrt{p}=2\Pi(1-r^b).$$

Nun setze man

$$\Pi(1-r^a) = L+M\Sigma r^a+N\Sigma r^b.$$

Hier bezeichnet also $L-1$ wie oft Null, M wie oft jeder Rest, N wie oft jeder Nichtrest in den geraden Classen der aus den Resten gebildeten Combinationen mehr vorkommt als in den ungeraden. Setzt man wieder für Σr^a und Σr^b ihre Werthe, so hat man

$$\Pi(1-r^a) = L-\frac{M+N}{2}+\frac{M-N}{2}\sqrt{p}$$

und mithin nach (17.)

$$(18.) \qquad 2L-(M+N)=y'; \qquad N-M=z'.$$

Bekanntlich enthalten aber die ungeraden Combinationsclassen, bei jeder Elementenzahl, eine Combination mehr als die geraden, man hat daher auch noch die Gleichung

$$L-1+(M+N)\frac{p-1}{2} = -1$$

oder

$$(19.) \qquad 2L+(M+N)(p-1) = 0.$$

Aus dieser Gleichung und der ersten Gleichung (18.) folgt zunächst

$$M+N = -\frac{y'}{p}.$$

Verbindet man diese Gleichung mit der zweiten Gleichung (18.) und setzt zugleich $y'=pt'$, so findet man mithin

$$(20.) \qquad \begin{cases} M = -\dfrac{t'+z'}{2}, \\ N = \dfrac{z'-t'}{2}, \\ L = \dfrac{p-1}{2}t'. \end{cases}$$

Durch diese Gleichungen ist also bei den Zahlen $p=4\nu+1$ der Unterschied der Vertheilung der Reste und Nichtreste unter den geraden und ungeraden Classen der aus den Resten gebildeten Combinationen vollkommen bestimmt.

Da $y_1^2-pz_1^2=4p$, also $z_1^2-pt_1^2=-4$, so folgt $z'>t'$, ausgenommen wenn $p=5$, wo $z'=t'=1$. Aus dem Werthe von N folgt also, dass die *Nichtreste* in den *geraden* Classen häufiger vorkommen als in den *ungeraden*, ausgenommen, wenn $p=5$. Dagegen zeigt der Werth von M, dass die *Reste* in den *ungeraden* Classen häufiger vorkommen als in den *geraden*. Zugleich zeigt der Werth von L, dass auch Null in den geraden Classen häufiger vor-

kommt als in den ungeraden, und dass die Differenz $L-1$ immer eine ungerade Zahl ist.

Für die Combinationen aus den Nichtresten erhält man ebenso aus

$$\Pi(1-r^b) = L'+M'\Sigma r^a+N'\Sigma r^b$$

die Gleichungen

$$M' = \frac{z'-t'}{2} = N,$$

$$N' = -\frac{z'+t'}{2} = M,$$

$$L' = \frac{p-1}{2}t' = L.$$

10. Die Erörterungen des vorhergehenden §. gelten gleichmässig für die Zahlen $8k+1$ wie für die Zahlen $8k+5$. Für die ersteren findet man nun durch die Verbindung der Gleichungen (15.) und (20.), wie oft jede Zahl in den geraden und in den ungeraden Combinationsclassen vorkommt.

Ist $p=8k+5$, so hat man

$$\Pi(1-r^a)\Pi(1+r^a) = \Pi(1-r^b).$$

Aus den Gleichungen (16.) und (17.) folgt daher

$$(y'-z'\sqrt{p})(Y_0+Z_0\sqrt{p}) = 2(y'+z'\sqrt{p}),$$

und da $Y_0=y_0$

$$y_1Y_0-z_1Z_0p = 2y',$$
$$y_1Z_0-Y_0z_1 = 2z'.$$

Mit Berücksichtigung der Gleichung $y_1^2-pz_1^2=4p$ ergiebt sich hieraus

$$Y_0 = \frac{y_1^2+pz_1^2}{2p} = \frac{z_1^2+pt_1^2}{2},$$

$$Z_0 = \frac{y'z'}{p} = t'z'.$$

Hier ist also Z_0 positiv und mithin gleich z_0, und daher

$$(21.) \quad \begin{cases} y_0+z_0\sqrt{p} = 2\Pi(1+r^a), \\ y_0-z_0\sqrt{p} = 2\Pi(1+r^b). \end{cases}$$

Setzt man nun wieder

$$\Pi(1+r^a) = l+m\Sigma r^a+n\Sigma r^b,$$

so findet man, indem man wie in §. 7 die Werthe von Σr^a und Σr^b substituirt,

$$2l-(m+n) = y_0,$$
$$m-n = z_0.$$

Verbindet man diese Gleichungen mit der Formel (13.), so erhält man

$$(22.)\quad \begin{cases} l = \dfrac{2^{\frac{1}{2}(p+1)} + (p-1)y_0}{2p}, \\ m = \dfrac{2^{\frac{1}{2}(p+1)} + pz_0 - y_0}{2p}, \\ n = \dfrac{2^{\frac{1}{2}(p+1)} - pz_0 - y_0}{2p}. \end{cases}$$

Die Werthe von l, m, n sind demnach durch Kreisfunctionen bestimmt.

Aus dem Werthe von l folgt

$$l-1 = \frac{2^{\frac{1}{2}(p+1)} - y_0 + (y_0-2)p}{2p},$$

die Zahl, welche angiebt, wie oft die Null unter den Combinationen aus den Resten vorkommt. Die Zahlen m und n können, ihrer Bedeutung nach, niemals negativ sein. Da nun $m-n = z_0$ und $z_0 = t'z'$ nicht Null sein kann, so kann m ebenfalls nicht Null sein und man hat daher jedenfalls $m > n$. Dies giebt den Satz:

Unter den Combinationen aus den Resten einer Primzahl von der Form $8k+5$ kommen die Reste in grösserer Anzahl vor als die Nichtreste.

Hierin unterscheiden sich also die Primzahlen dieser Form wesentlich von den übrigen Primzahlen, bei welchen, nach dem Vorhergehenden, Reste und Nichtreste immer in gleicher Zahl vorkommen.

Aus der Verbindung der Gleichungen (20.) und (22.) ergiebt sich wieder, wie oft jede Zahl in den geraden und in den ungeraden Combinationsclassen vorkommt.

11. Verfolgt man den von *Dirichlet* a. a. O. angegebenen Weg, so findet man noch folgende Resultate.

Ist $p = 8k+1$, so hat man nach Formel (14.)

$$\frac{\Pi(1+r^a)}{\Pi(1+r^b)} = 1 = \frac{\Pi\left(1+e^{\frac{2a\pi}{p}i}\right)}{\Pi\left(1+e^{\frac{2b\pi}{p}i}\right)}.$$

Entwickelt man $\log \dfrac{\Pi\left(1+e^{\frac{2a\pi}{p}i}\right)}{\Pi\left(1+e^{\frac{2b\pi}{p}i}\right)}$ in eine Reihe, so hat man mithin

$$\Sigma \frac{(-1)^{n-1}}{n}\left[\Sigma e^{\frac{2na\pi}{p}i} - \Sigma e^{\frac{2nb\pi}{p}i}\right] = 0,$$

wo sich die Summation in Beziehung auf n auf alle ganzen positiven Werthe von n bezieht. Da nun, wenn n kein Vielfaches von p ist,

$$(23.) \qquad \Sigma e^{\frac{2na\pi}{p}i} - \Sigma e^{\frac{2nb\pi}{p}i} = \left(\frac{n}{p}\right)\sqrt{p},$$

so folgt, dass für die Primzahlen $p = 8k+1$

$$\Sigma(-1)^{n-1}\left(\frac{n}{p}\right)\cdot\frac{1}{n} = 0,$$

wo die Werthe von n, die Vielfache von p sind, ausgeschlossen werden müssen. Dasselbe Resultat ergiebt sich, wenn $p = 8k+7$, da dann die Gleichung (23.) so wie (14.) statt hat.

Ist $p = 8k+5$, so ist

$$\Pi(1+r^a) = \frac{\Pi(1-r^b)}{\Pi(1-r^a)}; \qquad \Pi(1+r^b) = \frac{\Pi(1-r^a)}{\Pi(1-r^b)},$$

also nach Formel (3.)

$$\log\frac{\Pi(1+r^a)}{\Pi(1+r^b)} = 2\log\frac{\Pi(1-r^b)}{\Pi(1-r^a)} = 2\log\frac{\Pi\sin\frac{b\pi}{p}}{\Pi\sin\frac{a\pi}{p}}.$$

Dies ist mithin der Werth der Reihe $\sqrt{p}\,\Sigma(-1)^{n-1}\left(\frac{n}{p}\right)\frac{1}{n}$, wo wieder die Werthe von n, welche Vielfache von p sind, ausgeschlossen sind. Nun ist, wie *Dirichlet* a. a. O. gezeigt hat, $\log\frac{\Pi\sin\frac{b\pi}{p}}{\Pi\sin\frac{a\pi}{p}} = \sqrt{p}\,\Sigma\left(\frac{n}{p}\right)\frac{1}{n}$. Demnach ist für die Zahlen $p = 8k+5$ der Werth der Reihe $\Sigma(-1)^{n-1}\left(\frac{n}{p}\right)\frac{1}{n}$ das Doppelte des Werthes der Reihe $\Sigma\left(\frac{n}{p}\right)\frac{1}{n}$, sobald die Werthe von n, die Vielfache von p sind, ausgeschlossen werden.

Um den Werth von $\Sigma(-1)^{n-1}\left(\frac{n}{p}\right)\frac{1}{n}$ für den Fall, dass $p = 8k+3$ ist, zu bestimmen, kann man sich eines Verfahrens bedienen, welches *Dirichlet* ebenfalls in einem ähnlichen Falle angewandt hat und durch welches man den Werth der Reihe überhaupt für alle Zahlen $p = 4\nu+3$ erhält. Da nemlich bei dieser letzteren Zahlenform, für ein bestimmtes n, nach *Gauss*

$$\Sigma\sin\frac{2na\pi}{p} - \Sigma\sin\frac{2nb\pi}{p} = \left(\frac{n}{p}\right)\sqrt{p},$$

so hat man:

$$\sqrt{p}\,\Sigma(-1)^{n-1}\left(\frac{n}{p}\right)\frac{1}{n} = \Sigma\Sigma(-1)^{n-1}\sin\frac{2na\pi}{p}\cdot\frac{1}{n} - \Sigma\Sigma(-1)^{n-1}\sin\frac{2nb\pi}{p}\cdot\frac{1}{n},$$

wo man nun in der Doppelsumme für n *alle* ganzen Zahlen nehmen kann, da die Glieder, die sich auf Werthe von n beziehen, welche Vielfache von p sind, von selbst wegfallen.

Die Summation in Beziehung auf n kann vermittelst der Formel

$$\Sigma(-1)^{n-1}\frac{\sin nz}{n} = \operatorname{Arc\,tg}(\operatorname{tg}\tfrac{1}{2}z)$$

ausgeführt werden. In der ersten Doppelsumme ist $z=\frac{2a\pi}{p}$. Man bezeichne durch A_1 die *Summe* der Reste, welche kleiner als $\frac{1}{2}p$ sind, durch A_2 die *Summe* der Reste, die grösser als $\frac{1}{2}p$ sind. Da nun, wenn $a<\frac{1}{2}p$, mithin $z<\pi$ zugleich $\operatorname{Arc\,tg}(\operatorname{tg}\frac{1}{2}z)=\frac{1}{2}z=\frac{a\pi}{p}$, so wird der auf diese a bezügliche Theil der ersten Doppelsumme $=A_1\frac{\pi}{p}$. Ist dagegen $a>\frac{1}{2}p$, also $z>\pi$, und man setzt $z=2\pi-\varphi$, so ist $\operatorname{Arc\,tg}(\operatorname{tg}\frac{1}{2}z)=-\frac{1}{2}\varphi=\frac{a\pi}{p}-\pi$, und der auf diese a bezügliche Theil der ersten Doppelsumme wird $A_2\frac{\pi}{p}-s\pi$, wo s die *Anzahl* der a, die grösser als $\frac{1}{2}p$ sind, bedeutet. Bezeichnet man ferner durch B_1 die *Summe* der Nichtreste, die kleiner als $\frac{1}{2}p$ ist, durch B_2 die *Summe* der Nichtreste, die grösser als $\frac{1}{2}p$ ist, so ist die *Anzahl* der letzteren $\frac{1}{2}(p-1)-s$. Man hat daher:

$$\sqrt{p}\,\Sigma(-1)^{n-1}\left(\frac{n}{p}\right)\frac{1}{n} = \frac{\pi}{p}[A_1+A_2]-s\pi-\frac{\pi}{p}[B_1+B_2]+[\tfrac{1}{2}(p-1)-s]\pi.$$

Nun ist aber

$$A_2=sp-B_1, \qquad B_2=\left(\frac{p-1}{2}-s\right)p-A_1;$$

substituirt man diese Werthe, so findet man

$$\sqrt{p}\,\Sigma(-1)^{n-1}\left(\frac{n}{p}\right)\frac{1}{n} = 2(A_1-B_1)\frac{\pi}{p},$$

oder

$$\Sigma(-1)^{n-1}\left(\frac{n}{p}\right)\frac{1}{n} = 2(A_1-B_1)\frac{\pi}{p\sqrt{p}}.$$

Ist $p=8k+7$, so ist, wie oben gefunden wurde, der Werth der Reihe gleich Null, also muss in diesem Falle $A_1=B_1$ sein, ein schon bekanntes Resultat. Ist $p=8k+3$, so hat man, wie ebenfalls bekannt ist, $A_1-B_1=\Sigma b-\Sigma a$ *).

*) *Liouville* Journ. des Mathém. T. 7, p. 144.

In diesem Falle ist mithin

$$\Sigma(-1)^{n-1}\left(\frac{n}{p}\right)\frac{1}{n} = 2(\Sigma b - \Sigma a)\frac{\pi}{p\sqrt{p}};$$

in demselben Falle ist aber, wie *Dirichlet* bewiesen hat *),

$$\Sigma\left(\frac{n}{p}\right)\frac{1}{n} = (\Sigma b - \Sigma a)\frac{\pi}{p\sqrt{p}},$$

also wieder $\Sigma(-1)^{n-1}\left(\frac{n}{p}\right)\frac{1}{n}$ das Doppelte von $\Sigma\left(\frac{n}{p}\right)\frac{1}{n}$. Fasst man alle vier Fälle zusammen, so ergiebt sich allgemein:

$$\Sigma(-1)^{n-1}\left(\frac{n}{p}\right)\frac{1}{n} = \left[1-\left(\frac{2}{p}\right)\right]\Sigma\left(\frac{n}{p}\right)\frac{1}{n}.$$

*) Mathem. Abhandl. d. K. Ak. d. W. zu Berlin aus d. Jahre 1837, p. 56.

Göttingen, April 1862.