

Ueber die Functionen Y und Z , welche der Gleichung

$$\frac{4(x^p-1)}{x-1} = Y^2 + pZ^2 \text{ Genüge leisten, wo } p \text{ eine Primzahl der Form } 4k \pm 1 \text{ ist.}$$

(Von Herrn von Staudt in Erlangen.)

Die Untersuchungen, welche *Legendre* bereits im Jahre 1830 über obige Gleichung angestellt hat, sind dem Verfasser dieser Abhandlung erst vor Kurzem bekannt geworden, haben ihn jedoch von deren Veröffentlichung nicht abhalten können, da in derselben immer noch einiges Neue enthalten ist. Dahin gehören namentlich der Nachweis des Zusammenhangs, welchen die Coefficienten der Functionen Y, Z mit den durch f_m, φ_m, ψ_m bezeichneten Zahlen haben, dann die Aufstellung allgemeiner Formeln für jene Coefficienten und endlich der aus diesen Formeln abgeleitete einfache Beweis des Satzes, welcher in der Theorie der quadratischen Reste als Fundamentalsatz betrachtet wird.

1. Wenn a eine durch p nicht theilbare Zahl ist, so soll unter $\left(\frac{a}{p}\right)$, wie gewöhnlich, die positive oder negative Einheit verstanden werden, je nachdem a quadratischer Rest oder quadratischer Nichtrest der Primzahl p ist. Ist nun auch b eine durch p nicht theilbare Zahl, so ist bekanntlich $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

2. Zwischen 0 und p liegen $q = \frac{1}{2}(p-1)$ quadratische Reste

$$\alpha_1, \alpha_2, \alpha_3, \dots \alpha_q$$

und eben so viele quadratische Nichtreste

$$\beta_1, \beta_2, \beta_3, \dots \beta_q$$

der Zahl p . Ist nun h eine durch p nicht theilbare Zahl und zwar quadratischer Rest, so kann man überall, wo jede von zwei congruenten Zahlen die Stelle der andern vertreten kann, statt des Systems $h(\alpha)$ von Zahlen, welches nämlich aus den Producten $h\alpha_1, h\alpha_2, h\alpha_3, \dots h\alpha_q$ besteht, das System (α) und eben so statt des Systems $h(\beta)$ das System (β) setzen, während, wenn h quadratischer Nichtrest ist, (β) für $h(\alpha)$ und (α) für $h(\beta)$ gesetzt werden kann. So wie hier, so hat man auch in der Folge, wenn nicht aus-

drücklich ein anderer Modulus genannt wird, die Primzahl p als Modulus zu betrachten.

3. Wenn $p > 3$ ist und also wenigstens ein quadratischer Rest h zwischen 1 und p liegt, so ist sowohl die Summe der Zahlen (α) als auch die Summe der Zahlen (β) der Null congruent. Wird nämlich irgend eine dieser Summen durch s bezeichnet, so ist $hs \equiv s$, woraus der Satz folgt.

4. Bezeichnet man das Product aus den Zahlen (α) durch P_α , das Product aus den Zahlen (β) aber durch P_β , so ist

$$P_\beta \equiv \left(\frac{-1}{p}\right) \equiv -P_\alpha.$$

Zu jedem zwischen 1 und $p-1$ liegenden Factor x sowohl des einen als auch des anderen Products giebt es einen zwischen denselben Grenzen liegenden Factor y desselben Products, so dass $xy \equiv 1$ ist. Setzt man für je zwei solche Factoren die Einheit, so folgt, dass entweder $P_\beta \equiv 1 \equiv -P_\alpha$ oder $P_\alpha \equiv 1 \equiv -P_\beta$ ist, je nachdem nämlich die Zahl $p-1$ unter den Zahlen (α) oder unter den Zahlen (β) sich befindet. Aus dem Satze geht noch hervor, dass $(p-1)! \equiv -1$ ist.

5. Ist h irgend eine durch p nicht theilbare Zahl, so ist

$$h^q \equiv \left(\frac{h}{p}\right).$$

Das Product $h^q P_\alpha$ aus den Zahlen $h(\alpha)$ ist nämlich dem Producte P_α oder dem Producte P_β congruent, je nachdem h quadratischer Rest oder quadratischer Nichtrest ist. Im erstern dieser Fälle ist also $h^q \equiv 1$, im letztern aber, da $P_\beta \equiv -P_\alpha$ ist, $h^q \equiv -1$.

Namentlich ist $\left(\frac{-1}{p}\right) = (-1)^q$ und mithin -1 quadratischer Rest oder quadratischer Nichtrest der Zahl p , je nachdem q eine pare oder eine unpare Zahl ist, oder je nachdem p die Form $4k+1$ oder $4k-1$ hat.

6. Versteht man unter q_m den Ausdruck $\frac{q(q-1)(q-2)\dots(q-m+1)}{1.2.3\dots m}$, so giebt es $q_m \cdot q_n$ Summen, deren jede aus m Zahlen des Systems (α) und n Zahlen des Systems (β) besteht. Bezeichnet man ferner die Anzahl derjenigen dieser Summen, welche der Zahl a congruent sind, durch (m, n, a) , so ist

$$(m, n, 0) + (m, n, 1) + (m, n, 2) + \text{etc.} \dots + (m, n, p-1) = q_m \cdot q_n.$$

Es wird hier vorausgesetzt, dass keine der beiden Zahlen m, n negativ und höchstens eine derselben Null sei, in welchem Falle 1 für q_0 zu setzen ist.

Von den q_m Summen, deren jede aus m Zahlen des Systems (α) besteht, sind $(m, 0, a)$, von den q_n Summen aber, deren jede aus n Zahlen des Systems (β) besteht, $(0, n, a)$ der Zahl a congruent. Ist irgend eine der Zahlen m, n grösser als q , so ist, was auch a für eine Zahl sein mag, $(m, n, a) = 0$ und eben so $q_m \cdot q_n = 0$.

7. Schreibt man statt (m, n, a) , im Falle $a \equiv 0$ ist, nur $f(m, n)$, so hat man die Gleichung:

$$f(m, n) = f(n, m).$$

Nach der eingeführten Bezeichnung giebt es nämlich $f(m, n)$ der Null congruente Summen, deren jede aus m Zahlen des Systems (α) und n Zahlen des Systems (β) besteht. Multiplicirt man nun alle diese Summen mit einem und demselben quadratischen Nichtreste h und setzt dann statt der Summanden $h\alpha_1, h\alpha_2, h\alpha_3, \dots$ die ihnen congruenten Zahlen des Systems (β) und statt der Summanden $h\beta_1, h\beta_2, h\beta_3, \dots$ die ihnen congruenten Zahlen des Systems (α) , so hat man $f(m, n)$ der Null congruente Summen, deren jede aus n Zahlen des Systems (α) und m Zahlen des Systems (β) besteht, woraus der Satz folgt.

8. Wenn a, b zwei durch p nicht theilbare Zahlen sind, so ist entweder $(m, n, a) = (m, n, b)$ oder $(m, n, a) = (n, m, b)$, je nachdem nämlich $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ oder $\left(\frac{a}{p}\right) = -\left(\frac{b}{p}\right)$ ist.

Es sei $b \equiv ha$. Da es nun (m, n, a) der Zahl a congruente Summen giebt, deren jede aus m Zahlen des Systems (α) und n Zahlen des Systems (β) besteht, so giebt es auch (m, n, a) der Zahl b congruente Summen, deren jede aus m Zahlen des Systems $h(\alpha)$ und n Zahlen des Systems $h(\beta)$ besteht. Setzt man für jeden Summanden seinen kleinsten positiven Rest, so erhält man (m, n, a) der Zahl b congruente Summen, deren jede, wenn h quadratischer Rest ist, aus m Zahlen des Systems (α) und n Zahlen des Systems (β) , im entgegengesetzten Falle aber aus n Zahlen des Systems (α) und m Zahlen des Systems (β) besteht, woraus der Satz folgt.

9. Schreibt man $\varphi(m, n)$ statt $(m, n, 1)$, so ist nach dem Vorigen, wenn a eine durch p nicht theilbare Zahl bezeichnet, $(m, n, a) = \varphi(m, n)$ oder $= \varphi(n, m)$, je nachdem a quadratischer Rest oder quadratischer Nichtrest der Zahl p ist. Die in 6. aufgestellte Gleichung aber geht nun in folgende über:

$$f(m, n) + q\varphi(m, n) + q\varphi(n, m) = q_m \cdot q_n.$$

Für $p = 7$ wird $f(1, 2) = 0$, $\varphi(1, 2) = 1$, $\varphi(2, 1) = 2$.

10. Setzt man im Vorigen $n = m$, so ergibt sich die Gleichung:

$$f(m, m) + 2q\varphi(m, m) = q_m \cdot q_m.$$

Namentlich ist also

$$f(1, 1) + 2q\varphi(1, 1) = q^2.$$

11. Ist x eine Zahl des Systems (α) , so ist $p - x$ eine Zahl des Systems (α) oder des Systems (β) , je nachdem q eine pare oder eine unpare Zahl ist. Im erstern dieser Fälle ist $f(2, 0) = \frac{1}{2}q$, $f(1, 1) = 0$, folglich $\varphi(1, 1) = \frac{1}{2}q = \frac{1}{4}(p-1)$ und mithin $1 - 4f(1, 1) + 4\varphi(1, 1) = p$, während im letztern Falle $f(2, 0) = 0$, $f(1, 1) = q$, folglich $\varphi(1, 1) = \frac{1}{2}(q-1) = \frac{1}{4}(p-3)$ und mithin $1 - 4f(1, 1) + 4\varphi(1, 1) = -p$ ist.

12. Schreibt man f_m statt $f(m, 0)$, φ_m statt $\varphi(m, 0)$ und ψ_m statt $\varphi(0, m)$, so folgt aus 9., wenn man daselbst $n = 0$ setzt

$$f_m + q\varphi_m + q\psi_m = q_m.$$

Unter den q_m Summen, deren jede aus m Zahlen des Systems (α) besteht, sind f_m der Null, φ_m der Einheit und $\psi_m = (0, m, 1) = (m, 0, h)$ einem und demselben quadratischen Nichtreste h congruent. Ist $p = 13$, so ist $f_2 = 3$, $\varphi_2 = 1$, $\psi_2 = 1$.

13. Setzt man

$$\begin{aligned} 2f_m - \varphi_m - \psi_m &= (-1)^m C_m, \\ -\varphi_m + \psi_m &= (-1)^m D_m, \end{aligned}$$

so wird

$$C_m + D_m = 2(-1)^m (f_m - \varphi_m),$$

woraus man schliessen kann, dass C_m , D_m entweder zwei pare oder zwei unpare Zahlen sind. Verbindet man die obigen Gleichungen mit der in der vorigen Nummer enthaltenen, so findet man

$$\begin{aligned} pf_m &= q_m + q(-1)^m C_m, \\ p\varphi_m + p\psi_m &= 2q_m - (-1)^m C_m, \\ 2p\varphi_m &= 2q_m - (-1)^m C_m - p(-1)^m D_m, \\ 2p\psi_m &= 2q_m - (-1)^m C_m + p(-1)^m D_m. \end{aligned}$$

Aus diesen Gleichungen geht hervor, dass $(-1)^m C_m \equiv 2q_m$ ist.

14. Da $f_1 = 0$, $\varphi_1 = 1$, $\psi_1 = 0$, so ist $C_1 = D_1 = 1$. Ist $p = 3$ und also $q = 1$, so ist auch $f_q = 0$, $\varphi_q = 1$, $\psi_q = 0$ und $C_q = D_q = 1$. Wenn aber $p > 3$ und also die Summe der Zahlen (α) der Null congruent ist, so ist $f_q = 1$, $\varphi_q = \psi_q = 0$, mithin $C_q = 2(-1)^q$ und $D_q = 0$.

15. Wenn m zwischen 0 und q liegt und $n = q - m$ ist, so ist $f_m = f_n$ und überdies

entweder $\varphi_m = \varphi_n$ und $\psi_m = \psi_n$

oder $\varphi_m = \psi_n$ und $\psi_m = \varphi_n$,

je nachdem nämlich q eine pare oder unpare Zahl ist. Wenn nämlich eine Summe, welche aus m Zahlen des Systems (α) besteht, der Zahl a congruent ist, so ist die Summe der n übrigen Zahlen desselben Systems $\equiv -a$, woraus man schliessen kann, dass $(m, 0, a) = (n, 0, -a)$ und eben so $(0, m, a) = (0, n, -a)$ ist. Setzt man $a = 0$, so folgt, dass $f_m = f_n$ ist. Setzt man $a = 1$, so erhält man die Gleichungen:

$$\varphi_m = (n, 0, -1), \quad \psi_m = (0, n, -1).$$

Nun ist nach 9., wenn -1 quadratischer Rest der Zahl p ist, $(n, 0, -1) = (n, 0, 1) = \varphi_n$ und $(0, n, -1) = (0, n, 1) = \psi_n$, im entgegengesetzten Falle aber $(n, 0, -1) = (0, n, 1) = \psi_n$ und $(0, n, -1) = (n, 0, 1) = \varphi_n$, woraus der Satz sich ergibt.

Aus dem obigen Satze und aus 13. folgt noch, dass $(-1)^m C_m = (-1)^n C_n$ und $(-1)^m D_m = (-1)^{n+q} D_n$ ist. Multiplicirt man auf beiden Seiten mit $(-1)^m$, so ergeben sich die Gleichungen:

$$C_m = (-1)^q C_n, \quad D_m = D_n.$$

16. Bezeichnet ω eine imaginäre Wurzel der Gleichung $x^p - 1 = 0$, so ist

$$1 + \omega + \omega^2 + \omega^3 + \text{etc.} \dots + \omega^{p-1} = 0.$$

Sind ferner m, n irgend zwei Zahlen, so ist, wenn $m \equiv n$ ist, $\omega^m = \omega^n$. Ist aber $m - n$ durch p nicht theilbar, so sind ω^m, ω^n zwei verschiedene Wurzeln der Gleichung $x^p - 1 = 0$ und daher die Glieder der obigen Summe die p Wurzeln derselben. Setzt man also

$$(x - \omega^{\alpha_1})(x - \omega^{\alpha_2}) \dots (x - \omega^{\alpha_q}) = U,$$

$$(x - \omega^{\beta_1})(x - \omega^{\beta_2}) \dots (x - \omega^{\beta_q}) = V,$$

so ist

$$\frac{x^p - 1}{x - 1} = UV.$$

17. Bezeichnet man die Summe der Potenzen $\omega^{\alpha_1}, \omega^{\alpha_2}, \dots \omega^{\alpha_q}$ durch A_1 , die Summe der Producte aus je zweien derselben durch A_2 , die Summe der Producte aus je dreien durch A_3 u. s. w. und eben so die Summe der Potenzen $\omega^{\beta_1}, \omega^{\beta_2}, \dots \omega^{\beta_q}$ durch B_1 , die Summe der Producte aus je zweien derselben durch B_2 , die Summe der Producte aus je dreien durch B_3 u. s. w.,

so ist

$$U = x^q - A_1 x^{q-1} + A_2 x^{q-2} - \text{etc.} \dots \pm A_q,$$

$$V = x^q - B_1 x^{q-1} + B_2 x^{q-2} - \text{etc.} \dots \pm B_q.$$

18. Wenn man die Summe A_m mit der Summe B_n multiplicirt, so erhält man eine Summe von $q_m \cdot q_n$ Potenzen und zwar jede Potenz von ω , deren Exponent von m Zahlen des Systems (α) und n Zahlen des Systems (β) die Summe ist. Fasst man nun solche Potenzen, welche, weil ihre Exponenten congruent, einander gleich sind, zusammen, so folgt:

$$A_m \cdot B_n = f(m, n) + (m, n, 1) \omega + (m, n, 2) \omega^2 + \text{etc.} \dots + (m, n, p-1) \omega^{p-1}.$$

Da aber, wenn α eine Zahl des Systems (α) und β eine Zahl des Systems (β) bezeichnet, $(m, n, \alpha) = \varphi(m, n)$ und $(m, n, \beta) = \varphi(n, m)$ ist, so geht die obige Gleichung in nachstehende über:

$$A_m B_n = f(m, n) + \varphi(m, n) A_1 + \varphi(n, m) B_1.$$

19. Nach 16. ist $A_1 + B_1 = -1$. Setzt man also $-A_1 + B_1 = \varrho$, so wird $2A_1 = -1 - \varrho$, $2B_1 = -1 + \varrho$ und mithin $\varrho^2 = 1 - 4A_1 B_1$. Nun ist nach dem vorigen Satze, wenn daselbst $m = n = 1$ gesetzt wird, $A_1 B_1 = f(1, 1) - \varphi(1, 1)$, woraus hervorgeht, dass $\varrho^2 = 1 - 4f(1, 1) + 4\varphi(1, 1) = \pm p$ ist, wo das obere oder untere Zeichen gilt, je nachdem (11.) die Primzahl p die Form $4k+1$ oder $4k-1$ hat.

20. Setzt man in der vorletzten Nummer $n = 0$ und also 1 statt B_n , so erhält man die Gleichung:

$$A_m = f_m + \varphi_m A_1 + \psi_m B_1.$$

Multiplicirt man auf beiden Seiten mit 2 und setzt alsdann $-1 - \varrho$ statt $2A_1$ und $-1 + \varrho$ statt $2B_1$, so folgt

$$2A_m = 2f_m - \varphi_m - \psi_m + (\psi_m - \varphi_m) \varrho.$$

Wenn man endlich auch noch mit $(-1)^m$ multiplicirt, so erhält man

$$2(-1)^m A_m = C_m + D_m \varrho.$$

Eben so findet man, wenn man in 18. zuerst m mit n vertauscht und dann $n = 0$ setzt:

$$2B_m = f_m + \psi_m A_1 + \varphi_m B_1,$$

$$2(-1)^m B_m = C_m - D_m \varrho.$$

21. Setzt man

$$2x^q + C_1 x^{q-1} + C_2 x^{q-2} + \text{etc.} \dots + C_q = Y,$$

$$D_1 x^{q-1} + D_2 x^{q-2} + \text{etc.} \dots + D_q = Z,$$

so wird nach 17. und 20.

$$2U = Y + \varrho Z,$$

$$2V = Y - \varrho Z,$$

mithin

$$\frac{4(x^p - 1)}{x - 1} = Y^2 \mp pZ^2,$$

wo das obere oder untere Zeichen gilt, je nachdem p die Form $4k+1$ oder $4k-1$ hat. Setzt man $p=3$, so folgt

$$\frac{4(x^3 - 1)}{x - 1} = (2x + 1)^2 + 3.$$

Ist aber $p > 3$, so ist nach 14. und 15.

$$C_q = 2(-1)^q, \quad D_q = 0$$

und, wenn m zwischen 0 und q liegt,

$$C_{(q-m)} = (-1)^q \cdot C_m, \quad D_{(q-m)} = D_m.$$

22. Da es sehr mühsam ist, für grosse Werthe von m und p die Werthe von f_m , φ_m und ψ_m zu finden, um dann aus ihnen die Werthe von C_m und D_m zu berechnen, so ist ein Verfahren wünschenswerth, durch welches die letztern unmittelbar gefunden werden. Auf ein solches Verfahren führt aber nachstehender Satz:

Bezeichnet man die Summe der q Unbestimmten $\omega_1, \omega_2, \omega_3, \dots \omega_q$ durch A_1 , die Summe der Producte aus je zweien derselben durch A_2 , die Summe der Producte aus je dreien durch A_3 u. s. w. und die Summe der Potenzen $\omega_1^h, \omega_2^h, \omega_3^h, \dots \omega_q^h$ durch S_h , so ist

$$A_m = (-1)^m \Sigma \frac{(-S_1)^a}{a! 1^a} \cdot \frac{(-S_2)^b}{b! 2^b} \cdot \frac{(-S_3)^c}{c! 3^c} \dots,$$

$$a + 2b + 3c + \text{etc.} = m,$$

woraus zugleich hervorgeht, dass A_m durch die Summen $S_1, S_2, S_3, \dots S_m$ bestimmt ist.

23. Setzt man im Vorigen statt der Unbestimmten $\omega_1, \omega_2, \dots \omega_q$ die Potenzen $\omega^{\alpha_1}, \omega^{\alpha_2}, \dots \omega^{\alpha_q}$ der Imaginären ω , so wird S_h , im Falle h durch p theilbar ist, $= q$, im entgegengesetzten Falle aber $= A_1 = \frac{1}{2}(-1 - \varrho)$ oder $= B_1 = \frac{1}{2}(-1 + \varrho)$, je nachdem $\left(\frac{h}{p}\right) = 1$ oder $= -1$ ist. Da nun A_m für alle Werthe von m , welche $> q$ sind, Null wird, also für solche Werthe nicht erst zu berechnen ist, so kann man annehmen, dass $m < p$ sei. In diesem Falle ist aber, wenn S_h in A_m vorkommt, auch $h < p$ und mithin

$-S_h = \frac{1}{2}(1 + \varrho \lambda_h)$, wo der Einfachheit wegen λ_h für $\left(\frac{h}{p}\right)$ geschrieben ist. Die in der vorigen Nummer aufgestellte Gleichung geht hiernach, wenn auf beiden Seiten noch mit $2(-1)^m$ multiplicirt wird, in nachstehende über:

$$C_m + D_m \varrho = 2 \sum \frac{(1 + \varrho \lambda_1)^a}{a! 2^a} \cdot \frac{(1 + \varrho \lambda_2)^b}{b! 4^b} \cdot \frac{(1 + \varrho \lambda_3)^c}{c! 6^c} \dots$$

$$a + 2b + 3c + \text{etc.} = m.$$

Der Ausdruck rechter Hand kann, wenn man ihn zuerst nach Potenzen von ϱ entwickelt und alsdann, weil $\varrho^2 = (-1)^q p$ ist, $(-1)^{nq} \cdot p^n$ statt ϱ^{2n} und $(-1)^{nq} \cdot p^n \varrho$ statt ϱ^{2n+1} setzt, in die Form $P + Q\varrho$ gebracht werden, wo P , Q von ϱ frei sind. Weil aber ϱ entweder irrational oder imaginär ist, so hat man die beiden Gleichungen:

$$C_m = P, \quad D_m = Q.$$

24. Setzt man im Vorigen $m = 1$ und dann auch $m = 2$, so erhält man die Gleichungen

$$C_1 + D_1 \varrho = 1 + \varrho,$$

$$C_2 + D_2 \varrho = \frac{1}{4}(1 + \varrho)^2 + \frac{1}{2}(1 + \varrho \lambda_2).$$

Aus der erstern folgt, dass $C_1 = D_1 = 1$ ist; aus der letztern folgt:

$$C_2 = \frac{1}{4}(3 + \varrho^2), \quad D_2 = \frac{1}{2}(1 + \lambda_2).$$

Ist nun $p = 4k \pm 1$, so ist $\varrho^2 = 1 \pm 4k$, $C_2 = 1 \pm k$. Da endlich C_2 , D_2 nach 13. entweder zwei unpare oder zwei pare Zahlen sind, so ist $\lambda_2 = 1$ und $D_2 = 1$ oder $\lambda_2 = -1$ und $D_2 = 0$, je nachdem k eine pare oder unpare Zahl ist. Die Zahl 2 ist also quadratischer Rest oder quadratischer Nichtrest der Primzahl p , je nachdem diese die Form $8n \pm 1$ oder die Form $8n \pm 3$ hat.

25. Ist $m = 2n + 1$ eine unpare Primzahl, so kann, wie man sich leicht überzeugt, C_m in die Form $\frac{1}{m! 2^{m-1}} + \frac{1}{m} + G$, D_m aber in die Form $\frac{(-1)^{nq} \cdot p^n}{m! 2^{m-1}} + \frac{\lambda_m}{m} + H$ gebracht werden, wo G , H Brüche sind, deren Nenner den Factor m nicht enthalten. Da nun C_m , D_m ganze Zahlen sind, so muss sowohl $1 + (m-1)! 2^{m-1}$, als auch $(-1)^{nq} \cdot p^n + (m-1)! 2^{m-1} \cdot \lambda_m$, mithin auch, wenn man die erstere Summe mit $\left(\frac{m}{p}\right) = \lambda_m$ multiplicirt und sie alsdann von der letztern abzieht, $(-1)^{nq} \cdot p^n - \left(\frac{m}{p}\right)$ durch m theilbar sein. Da endlich, wie aus 5. hervorgeht, wenn man daselbst m statt p und p statt h setzt, auch $p^n - \left(\frac{p}{m}\right)$ durch m theilbar ist, so ist auch $(-1)^{nq} \cdot \left(\frac{p}{m}\right) - \left(\frac{m}{p}\right)$ durch m theilbar,

woraus man schliessen kann, dass $\left(\frac{m}{p}\right) = (-1)^{n_2} \left(\frac{p}{m}\right)$, mithin, wenn man auf beiden Seiten noch mit $\left(\frac{p}{m}\right)$ multiplicirt, $\left(\frac{m}{p}\right) \left(\frac{p}{m}\right) = (-1)^{n_2}$ ist.

26. Setzt man in der in 23. aufgestellten Gleichung $m = 3$, so folgt, wenn $p > 3$ ist,

$$C_3 + D_3 \varrho = \frac{(1+\varrho)^3}{24} + \frac{(1+\varrho)(1+\varrho\lambda_2)}{4} + \frac{1+\varrho\lambda_3}{3},$$

woraus sich die beiden Gleichungen ergeben:

$$C_3 = \frac{1 \pm 3p}{24} + \frac{1 \pm p\lambda_2}{4} + \frac{1}{3} = \frac{5 \pm p(1+2\lambda_2)}{8},$$

$$D_3 = \frac{3 \pm p}{24} + \frac{1 + \lambda_2}{4} + \frac{\lambda_3}{3} = \frac{9 + 6\lambda_2 + 8\lambda_3 \pm p}{24},$$

wo die oberen oder unteren Zeichen gelten, je nachdem p die Form $4k+1$ oder die Form $4k-1$ hat. Ist also $p = 8n \pm 1$, so ist $C_3 = \frac{5+3(1 \pm 8n)}{8} = 1 \pm 3n$. Ist aber $p = 8n \mp 3$, so ist $C_3 = \frac{5+3 \mp 8n}{8} = 1 \mp n$.

27. Wird m als gegeben betrachtet, so sind C_m , D_m ganze Functionen von p und zwar ist, wenn m eine pare Zahl ist, die erstere vom Grade $\frac{1}{2}m$, die letztere aber vom Grade $\frac{1}{2}m-1$, während, wenn m eine unpare Zahl ist, beide vom Grade $\frac{1}{2}(m-1)$ sind. Weil aber die Coefficienten von C_m selbst wieder von den Einheiten $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, $\left(\frac{3}{p}\right)$, ... $\left(\frac{m-1}{p}\right)$ abhängen, so ist C_m nur für alle diejenigen Werthe von p eine und dieselbe Function von p , welche, wenn man das Product aus allen Primzahlen, die kleiner als m sind, durch P_m bezeichnet, nach dem Modulus $4P_m$ congruent sind. Eben so ist, wenn man das Product aus allen Primzahlen, deren keine grösser als m ist, durch Q_m bezeichnet, D_m für alle Werthe von p , welche nach dem Modulus $4Q_m$ congruent sind, eine und dieselbe Function von p . Wenn nämlich die Differenz zweier Primzahlen p_1 , p_2 sowohl durch 8 als auch durch jeden Primfactor der Zahl h theilbar ist, so ist, wie man sich leicht überzeugt, $\left(\frac{h}{p_1}\right) = \left(\frac{h}{p_2}\right)$. Dass $\left(\frac{-1}{p_1}\right) = \left(\frac{-1}{p_2}\right)$ ist, geht schon daraus hervor, weil $p_1 - p_2$ durch 4 theilbar ist, mithin die Zahlen p_1 , p_2 entweder beide die Form $4k+1$ oder beide die Form $4k-1$ haben.

Ist $m = 3$, so ist $4Q_m = 24$, daher man bei der Bestimmung von D_3 zu unterscheiden hat, welcher von 8 zwischen -12 und $+12$ liegenden Zahlen ± 1 , ± 5 , ∓ 7 , ∓ 11 die Primzahl p nach dem Modulus 24 congruent ist. Ist

$p = 24n - 7$, so ist $\left(\frac{-1}{p}\right) = 1$, $\left(\frac{2}{p}\right) = 1$, $\left(\frac{3}{p}\right) = -1$, folglich $D_3 = \frac{9+6-8+p}{24} = \frac{7+p}{24} = n$.

28. Wenn die Summe zweier Primzahlen p_1, p_2 sowohl durch 8 als auch durch jeden Primfactor der positiven Zahl h theilbar ist, so ist $\left(\frac{h}{p_1}\right) = \left(\frac{h}{p_2}\right)$, während $\left(\frac{-1}{p_1}\right) = -\left(\frac{-1}{p_2}\right)$ ist.

Hat nämlich p_1 die Form $8n \pm 1$, so hat p_2 die Form $8n \mp 1$. Hat aber p_1 die Form $8n \pm 3$, so hat p_2 die Form $8n \mp 3$, daher in jedem Falle $\left(\frac{2}{p_1}\right) = \left(\frac{2}{p_2}\right)$ ist. Ist h eine unpare Primzahl, so ist $\left(\frac{p_1}{h}\right) = \left(\frac{p_2}{h}\right)$ oder $\left(\frac{p_1}{h}\right) = -\left(\frac{p_2}{h}\right)$, je nachdem h die Form $4k+1$ oder $4k-1$ hat. Da nun im erstern Falle auch $\left(\frac{p_1}{h}\right)\left(\frac{h}{p_1}\right) = \left(\frac{p_2}{h}\right)\left(\frac{h}{p_2}\right)$, im letztern Falle aber, weil die eine von den Zahlen p_1, p_2 die Form $4k+1$ und die andere die Form $4k-1$ hat, $\left(\frac{p_1}{h}\right)\left(\frac{h}{p_1}\right) = -\left(\frac{p_2}{h}\right)\left(\frac{h}{p_2}\right)$ ist, so ist in jedem Falle $\left(\frac{h}{p_1}\right) = \left(\frac{h}{p_2}\right)$. Da hiernach der Satz gilt, wenn h eine Primzahl ist, durch welche $p_1 + p_2$ getheilt werden kann, so gilt er auch nach 1., wenn h ein Product aus solchen Primzahlen ist.

29. Bei der Bestimmung von C_m , hat man zu unterscheiden, welcher von den zwischen $-2P_m$ und $+2P_m$ liegenden Zahlen, deren keine mit P_m einen gemeinschaftlichen Theiler hat, die Primzahl p nach dem Modulus $4P_m$ congruent ist. Wenn nun r eine jener Zahlen ist und für $p = 4nP_m + r$

$$C_m = F(p) = F(r + 4nP_m) = \Phi(n)$$

ist, so ist für $p = 4nP_m - r$

$$C_m = F(-p) = F(r - 4nP_m) = \Phi(-n).$$

Nach dem vorigen Satze hat nämlich, was auch h für eine zwischen 0 und m liegende Zahl sein mag, $\left(\frac{h}{p}\right)$ in beiden Fällen einen und denselben Werth. Bemerkt man nun noch, dass in dem einen von den beiden Fällen p die Form $4k+1$ hat und also $\varrho^2 = p$ ist, während im andern p die Form $4k-1$ hat und also $\varrho^2 = -p$ ist, so folgt der Satz. Eben so lässt sich nachstehender Satz beweisen:

Wenn r eine zwischen $-2Q_m$ und $+2Q_m$ liegende Zahl ist, welche mit Q_m keinen gemeinschaftlichen Theiler hat und für $p = 4nQ_m + r$

$$D_m = F(p) = \Phi(n)$$

ist, so ist für $p = 4nQ_m - r$

$$D_m = F(-p) = \Phi(-n).$$

Dass r zwischen den angegebenen Grenzen liege, ist für die obigen Sätze keine nothwendige Bedingung, sondern wurde nur deshalb angenommen, weil die Betrachtung dieser Fälle schon hinreichend ist.

30. Da $Q_3 = Q_4 = P_4 = P_5 = 6$ ist, so hat man bei den Bestimmungen von D_3 , D_4 , C_4 , C_5 nur zu unterscheiden, welche von den 8 Formen $24n+1$, $24n+5$, $24n+7$, $24n+11$ die Primzahl p hat. Die Fälle, in welchen die obern Zeichen gelten, und also p die Form $4k+1$ hat, finden sich in nachstehender Tafel. Setzt man in dieser statt $24n+r$, es mag r positiv oder negativ sein, $24n-r$ und zugleich in den unter D_3 , D_4 , C_4 , C_5 stehenden Functionen $-n$ statt n , so erhält man die den vier übrigen Fällen entsprechende Tafel.

p	D_3	D_4	C_4	C_5
$24n+1$	$n+1$	$2n+1$	$3n^2+11n+1$	$\frac{1}{2}5n^2+\frac{2}{2}5n+1$
$24n+5$	n	$-n$	$3n^2-2n$	$-\frac{9}{2}n^2+\frac{3}{2}n+1$
$24n-7$	n	$2n$	$3n^2+n$	$\frac{1}{2}5n^2-\frac{1}{2}n$
$24n-11$	n	$-n+1$	$3n^2+2n-1$	$-\frac{9}{2}n^2+\frac{1}{2}5n-2$

31. Da $Q_5 = Q_6 = P_6 = P_7 = 30$ ist, zwischen -60 und $+60$ aber 32 Zahlen liegen, deren keine mit 30 einen gemeinschaftlichen Theiler hat, so hat man bei den Bestimmungen von D_5 , D_6 , C_6 , C_7 32 Fälle zu unterscheiden. Nachstehende Tafel beschränkt sich auf die Functionen D_5 , D_6 , C_6 und enthält nur vier Fälle. Wie sich aber die Tafel für die erwähnten Functionen leicht vervollständigen lasse, ist weiter unten angegeben.

p	D_5	D_6	C_6
$120n+1$	$\frac{15}{2}n^2+\frac{29}{2}n+1$	$\frac{45}{2}n^2+\frac{37}{2}n+1$	$75n^3+\frac{5.127}{2}n^2+\frac{137}{2}n+1$
$120n-7$	$\frac{15}{2}n^2+\frac{7}{2}n$	$\frac{45}{2}n^2+\frac{1}{2}n$	$75n^3+\frac{5.41}{2}n^2+\frac{3}{2}n$
$120n-11$	$\frac{15}{2}n^2+\frac{11}{2}n$	$-15n^2+4n$	$75n^3+5.29n^2-9n$
$120n+29$	$\frac{15}{2}n^2+\frac{1}{2}n$	$-15n^2-n+1$	$75n^3+5.4n^2+11n+3$

Ist nun für $p = 120n + r$

$$D_5 = \Phi(n), \quad D_6 = \Phi_1(n), \quad C_6 = \Phi_2(n),$$

so ist (29.) für $p = 120n - r$

$$D_5 = \Phi(-n), \quad D_6 = \Phi_1(-n), \quad C_6 = \Phi_2(-n).$$

Wenn ferner $\frac{r_1 - r}{24} = \varepsilon$ eine ganze Zahl ist und $\left(\frac{r_1}{5}\right) - \left(\frac{r}{5}\right) = 2\delta$ gesetzt wird, so ist für $p = 120n + r_1$

$$D_5 = \Phi\left(n + \frac{\varepsilon}{5}\right) + \frac{2\delta}{5}, \quad D_6 = \Phi_1\left(n + \frac{\varepsilon}{5}\right) + \frac{\delta}{5}, \quad C_6 = \Phi_2\left(n + \frac{\varepsilon}{5}\right) \pm \delta\left(24n + \frac{r_1}{5}\right),$$

wo das obere oder untere Zeichen zu nehmen ist, je nachdem r_1 oder $-r_1$ die Form $4k+1$ hat. Man überzeugt sich von der Richtigkeit dieser Gleichungen, wenn man D_5 , D_6 , C_6 zuerst als Functionen von p darstellt und dann bemerkt, dass $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, $\left(\frac{3}{p}\right)$ dieselben Werthe haben, es mag $p = 120n + r$ oder $= 120n + r_1$ gesetzt werden.

Sucht man die Functionen D_5 , D_6 , C_6 für $p = 120n + 31$, so hat man $r_1 = 31$, für r aber diejenige von den Zahlen ± 1 , ∓ 7 , ∓ 11 , ± 29 , welche nach dem Modulus 24 der Zahl 31 congruent ist, nämlich die Zahl 7 zu setzen. Da alsdann $\varepsilon = 1$ und $\delta = 1$ wird und da für $p = 120n + 7$

$$D_5 = \frac{15}{2}n^2 - \frac{7}{2}n, \quad D_6 = \frac{45}{2}n^2 - \frac{1}{2}n, \quad C_6 = -75n^3 + \frac{5 \cdot 41}{2}n^2 - \frac{3}{2}n$$

ist, so ist für $p = 120n + 31$

$$D_5 = \frac{15}{2}\left(n + \frac{1}{5}\right)^2 - \frac{7}{2}\left(n + \frac{1}{5}\right) + \frac{2}{5} = \frac{15}{2}n^2 - \frac{1}{2}n,$$

$$D_6 = \frac{45}{2}\left(n + \frac{1}{5}\right)^2 - \frac{1}{2}\left(n + \frac{1}{5}\right) + \frac{1}{5} = \frac{45}{2}n^2 + \frac{17}{2}n + 1$$

$$\begin{aligned} C_6 &= -75\left(n + \frac{1}{5}\right)^3 + \frac{5 \cdot 41}{2}\left(n + \frac{1}{5}\right)^2 - \frac{3}{2}\left(n + \frac{1}{5}\right) - \left(24n + \frac{31}{5}\right) \\ &= -75n^3 + \frac{5 \cdot 23}{2}n^2 + \frac{13}{2}n - 3. \end{aligned}$$

32. Nach 13. kann man, wenn C_m , D_m bekannt sind, auch f_m , φ_m und ψ_m finden.

Ist $p = 8n \pm 1$, so ist $\varphi_2 = n - 1$, $\psi_2 = n$.

Ist $p = 8n + 4 \pm 1$, so ist $\varphi_2 = \psi_2 = n$.

33. Wenn z , $z+1$ zwei auf einander folgende Glieder der Reihe

$$1, \quad 2, \quad 3, \quad \dots \quad (p-1)$$

sind und $\left(\frac{z}{p}\right) = \left(\frac{z+1}{p}\right)$ ist, so soll gesagt werden, dass die Zahlen $z, z+1$ eine Folge I. oder II. Art bilden, je nachdem beide quadratische Reste oder quadratische Nichtreste der Zahl p sind. Ist aber $\left(\frac{z}{p}\right) = -\left(\frac{z+1}{p}\right)$, so soll $z, z+1$ ein Wechsel I. oder II. Art heissen, je nachdem die kleinere oder die grössere von den beiden Zahlen quadratischer Rest ist. Wenn man nun die Anzahl aller Folgen I. Art durch (R, R) , die Anzahl aller Wechsel I. Art durch (R, N) , die Anzahl aller Wechsel II. Art durch (N, R) und die Anzahl aller Folgen II. Art durch (N, N) bezeichnet und $p = 4k \pm 1$ setzt, so ist $(R, R) = k-1$, $(R, N) = k$, hingegen $(N, R) = (N, N) = k$ oder $= k-1$, je nachdem $p = 4k+1$ oder $= 4k-1$ ist.

Da nämlich die obige Reihe mit einem quadratischen Reste anfängt, so ist $(R, R) + (N, R) = \frac{1}{2}(p-3)$, während $(R, N) + (N, N) = \frac{1}{2}(p-1)$ ist. Da ferner nach 11. die Gleichung $x+y=p+1$, in welcher x eine Zahl des Systems (α) , y aber eine Zahl des Systems (β) sein soll, $\frac{1}{4}(p-1)$ oder $\frac{1}{4}(p-3)$ Auflösungen zulässt, je nachdem $p = 4k+1$ oder $= 4k-1$ ist, und da im erstern Falle $p-y, x$ ein Wechsel II. Art und $p-x, y$ ein Wechsel I. Art, im letztern Falle aber $p-y, x$ eine Folge I. Art und $p-x, y$ eine Folge II. Art ist, so ist im erstern Falle $(N, R) = (R, N) = \frac{1}{4}(p-1)$, folglich $(R, R) = \frac{1}{2}(p-3) - \frac{1}{4}(p-1) = \frac{1}{4}(p-5)$ und $(N, N) = \frac{1}{2}(p-1) - \frac{1}{4}(p-1) = \frac{1}{4}(p-1)$, im letztern aber $(R, R) = (N, N) = \frac{1}{4}(p-3)$, folglich $(N, R) = \frac{1}{2}(p-3) - \frac{1}{4}(p-3) = \frac{1}{4}(p-3)$ und $(R, N) = \frac{1}{2}(p-1) - \frac{1}{4}(p-3) = \frac{1}{4}(p+1)$, woraus der Satz sich ergibt *).

*) Leider habe ich die traurige Pflicht, den Lesern dieses Journals gleichzeitig mit dieser Abhandlung die Nachricht von dem Tode ihres hochverdienten Verfassers, dem dies Journal manchen werthvollen Beitrag verdankt, mittheilen zu müssen.

Georg Karl Christian von Staudt, 1798 zu Rothenburg an der Tauber geboren, einer der hervorragendsten Mathematiker aus der *Gauss'schen* Schule, seit 1835 Prof. ord. an der Universität zu Erlangen, starb am 1. Juni d. J., während er mit der Durchsicht der Correcturbogen der vorstehenden Abhandlung beschäftigt war. Seitdem er dieselbe vollendet und mir für das mathematische Journal zugesandt hatte, beschäftigte er sich mit geometrischen Untersuchungen und verfasste in den letzten drei Wochen seines Lebens eine Abhandlung „von den reellen und imaginären Halbmessern der Curven und Flächen zweiter Ordnung“, welche demnächst als besondere Schrift bei Korn in Nürnberg erscheinen soll. So hinterlässt der berühmte Verfasser der „Geometrie der Lage“ in seinen beiden letzten Arbeiten Untersuchungen aus den beiden Gebieten, denen er sich während seines Lebens immer mit besonderer Vorliebe gewidmet hatte, der Geometrie und der Theorie der Zahlen. B.