Zahlentheorie

Die Lehre von der Kreistheilung und ihre Beziehungen zur Zahlentheorie - academische Vorlesungen

Bachmann, Paul

Leipzig, 1872

ETH-Bibliothek Zürich

Persistent Link: https://doi.org/10.3931/e-rara-102738

Zwanzigste Vorlesung. Zwei Anwendungen auf die Theorie der quadratischen Formen.

Zwanzigste Vorlesung.

Zwei Anwendungen auf die Theorie der quadratischen Formen.

1. In der 10. und 11. Vorlesung sind wir aus der Kreistheilung zu verschiedenen Darstellungen von Primzahlen durch quadratische Formen geführt worden. Den Ausgangspunkt der dortigen Betrachtungen bildete ein eigenthümliches Verhalten, welches die Resolvante zeigt, wenn die Einheitswurzel durch eine entsprechende Congruenzwurzel ersetzt wird, ein Verhalten, welches in dem Nr. 2 der 10. Vorlesung ausgesprochenen Satze seinen Ausdruck fand. Hier wollen wir zwei weitere Anwendungen der Kreistheilung auf die Theorie der quadratischen Formen zusammenstellen, von welchen die erste, auf Formen bezüglich, deren Determinante eine negative ungerade Primzahl $-p$ sein soll, auf einer Verallgemeinerung der in der angeführten Stelle gegebenen Betrachtungen beruht*), während die zweite sich auf Formen von einer positiven Determinante, welche eine ungerade Primzahl $+p$ ist, bezieht und an die in Nr. 3 der 15. Vorlesung gefundene Zerlegung von $4X$ in zwei quadratische Factoren anzuknüpfen ist.**)

Wir werden im Folgenden mit $\psi(h, k, \omega)$ oder kürzer mit $\psi(h, k)$ den Ausdruck

$$\frac{(\omega^{-h}, R).(\omega^{-k}, R)}{(\omega^{-h-k}, R)}$$

bezeichnen, in welchem

$$(\omega^{-h}, R) = \sum_{\lambda=1}^{\lambda=q-1} \omega^{-h \operatorname{ind}.\lambda} . R^{\lambda}$$

ist, während R eine primitive Wurzel der Gleichung $x^q = 1$, ω eine primitive Wurzel der Gleichung $x^{q-1} = 1$ bedeuten soll; p und q seien ungerade Primzahlen, welche in der durch die Gleichung $q = \mu p + 1$ ausgedrückten Beziehung stehen, und unter γ werde wieder eine primitive Wurzel (mod. q) verstanden.

---

*) Vgl. hierzu Smith, report on the theory of numbres, art. 121. Auch Jacobi's Note über Kreistheilung und Cauchy, mém. sur la th. des nombres, besonders die Noten II, III und XIII.

**) S. Dirichlet, sur la manière de résoudre l'équation $t^2 - pu^2 = 1$ au moyen des fonctions circulaires, Cr. J. Bd. 17. Desgl. Jacobi's Note.

Jener Ausdruck hat folgende Eigenschaften, die hier sogleich zusammengestellt werden sollen:

1) Ist $h' \equiv h$, $k' \equiv k$ (mod. $q-1$), so ist offenbar $\psi(h', k') = \psi(h, k)$.

2) Ist eine der beiden Zahlen h, k z. B. h gleich Null, so wird der entsprechende Ausdruck $(\omega^{-h}, R) = (1, R)$ d. i. der Summe

$$R + R^2 + \ldots + R^{q-1}$$

gleich, deren Werth -1 ist, der andere Ausdruck (ω^{-k}, R) dem Nenner (ω^{-h-k}, R) gleich, also ist $\psi(0, k) = -1$, ebenso $\psi(h, 0) = -1$. Dasselbe gilt aber offenbar auch, wenn h und k Beide verschwinden, da dann jede der Functionen in dem Ausdrucke den Werth -1 annimmt; man findet demnach auch noch $\psi(0, 0) = -1$.

3) Wenn die Zahlen h, k nicht Null noch der Null mod. $(q-1)$ congruent sind und auch $h + k$ durch $q - 1$ nicht theilbar ist, so wird nach Nr. 5 der 8. Vorlesung der Ausdruck

$$(1) \quad \psi(h, k) = \frac{(\omega^{-h}, R) \cdot (\omega^{-k}, R)}{(\omega^{-h-k}, R)} = \sum_{\lambda=1}^{\lambda=q-2} \omega^{-h \operatorname{ind.} \lambda + (h+k) \operatorname{ind.} (1+\lambda)},$$

also einer ganzen Function von ω allein gleich. In diesem Falle ist bekanntlich

$$\psi(h, k) \cdot \psi(-h, -k) = \frac{(\omega^h, R)\,(\omega^{-h}, R) \cdot (\omega^k, R)\,(\omega^{-k}, R)}{(\omega^{h+k}, R)\,(\omega^{-h-k}, R)} = q$$

oder auch

$$(2) \qquad \psi(h, k) \cdot \psi(q-1-h, q-1-k) = q.$$

4) Ist $h + k$ durch $q - 1$ theilbar, ohne dass h oder k es sind, so nimmt der Ausdruck $\psi(h, k)$, da $k \equiv -h$ mod. $(q-1)$ und der Nenner $(\omega^{h+k}, R) = -1$ wird, die Form $-(\omega^h, R)(\omega^{-h}, R)$ an, und wird nach Formel (29) der 8. Vorlesung gleich $-(-1)^h \cdot q$, folglich ist

$$(3) \quad \psi(h, k) = (-1)^{h+1} \cdot q, \text{ wenn } h + k \equiv 0 \text{ mod. } (q-1).$$

2. Wir wollen nun unter $m_1, m_2, \ldots m_\alpha$ positive ganze Zahlen verstehen, welche kleiner als $q - 1$ vorausgesetzt werden sollen, und das Product

$$(\omega^{-m_1}, R) \cdot (\omega^{-m_2}, R) \ldots (\omega^{-m_\alpha}, R)$$

bilden. Dies kann offenbar durch ψ-Functionen ausgedrückt werden; denn man erhält zuerst

$$(\omega^{-m_1}, R) \cdot (\omega^{-m_2}, R) = \psi(m_1, m_2) \cdot (\omega^{-(m_1+m_2)}, R),$$

sodann, wenn mit μ_2 der kleinste positive Rest von $m_1 + m_2$ mod. $(q-1)$ bezeichnet wird, sodass $\mu_2 \equiv m_1 + m_2$ mod. $(q-1)$ ist,

$$(\omega^{-(m_1+m_2)}, R) \cdot (\omega^{-m_3}, R) = \psi(\mu_2, m_3) \cdot (\omega^{-(m_1+m_2+m_3)}, R),$$

ferner, wenn nun μ_3 den kleinsten positiven Rest von $m_1 + m_2 + m_3$ mod. $(q-1)$ bezeichnet,

$$(\omega^{-(m_1+m_2+m_3)}, R) \cdot (\omega^{-m_4}, R) = \psi(\mu_3, m_4) \cdot (\omega^{-(m_1+m_2+m_3+m_4)}, R)$$

u. s. w., endlich, wenn $\mu_{\alpha-1}$ der kleinste positive Rest von

$$m_1 + m_2 + \ldots + m_{\alpha-1} \text{ mod. } (q-1)$$

ist,

$$(\omega^{-(m_1+m_2+\ldots+m_{\alpha-1})}, R) \cdot (\omega^{-m_\alpha}, R)$$
$$= \psi(\mu_{\alpha-1}, m_\alpha) \cdot (\omega^{-(m_1+m_2+\ldots+m_\alpha)}, R).$$

Indem man alle diese Gleichungen in einander multiplicirt und die gemeinsamen Factoren beider Seiten weglässt, findet man folgende wichtige Formel:

(4) $(\omega^{-m_1}, R) \cdot (\omega^{-m_2}, R) \ldots (\omega^{-m_\alpha}, R) = \Psi(\omega) \cdot (\omega^{-(m_1+m_2+\ldots+m_\alpha)}, R)$,

in welcher

(5) $$\Psi(\omega) = \psi(m_1, m_2) \cdot \psi(\mu_2, m_3) \ldots \psi(\mu_{\alpha-1}, m_\alpha)$$

also eine ganze und ganzzahlige Function von ω allein ist, ebenso wie die Factoren aus denen es sich zusammensetzt. Betrachten wir nun diese Function etwas genauer.

Der allgemeine Factor $\psi(\mu_{i-1}, m_i)$ kann drei verschiedene Fälle darbieten, jenachdem

$\mu_{i-1} + m_i = q-1$, $\mu_{i-1} + m_i > q-1$, $\mu_{i-1} + m_i < q-1$

ist. Im letzten lassen wir ihn ungeändert, im ersten ersetzen wir ihn nach Gleichung (3) durch seinen Werth $(-1)^{1+\mu_{i-1}} \cdot q$, im zweiten schreiben wir dafür nach Gleichung (2)

$$\frac{q}{\psi(q-1-\mu_{i-1},\ q-1-m_i)},$$

in welchem Quotienten die ψ-Function des Nenners jetzt Argumente hat, die offenbar eine kleinere Summe ergeben, als $q-1$.

Es entsteht die Frage, wieoft einer der beiden ersten Fälle eintreten wird. Da μ_{i-1} der kleinste positive Rest ist, welchen die Summe

$$m_1 + m_2 + \ldots + m_{i-1}$$

durch $q-1$ getheilt lässt, kann man

$$m_1 + m_2 + \ldots + m_{i-1} = n_{i-1}(q-1) + \mu_{i-1}$$

setzen, indem man mit $n_{i-1}(q-1)$ das grösste, in der Summe enthaltene Vielfache von $(q-1)$ bezeichnet. Fügt man nun zu der Summe das folgende Glied m_i hinzu, und schreibt in analoger Weise

$$m_1 + m_2 + \ldots + m_{i-1} + m_i = n_i(q-1) + \mu_i,$$

während nun $n_i(q-1)$ das grösste darin enthaltene Vielfache von $q-1$ ist, so sind zwei Fälle zu unterscheiden: entweder ist $\mu_{i-1} + m_i < q-1$, dann wird $n_i = n_{i-1}$ sein müssen; oder aber es ist $\mu_{i-1} + m_i \geqq q-1$, dann wird offenbar $n_i = n_{i-1} + 1$, da $\mu_{i-1} + m_i$ eine Summe zweier Zahlen ist, welche kleiner als $q-1$ sind, — die erste als kleinster positiver Rest mod. $(q-1)$, die zweite nach der Voraussetzung — deren Summe also jedenfalls $2(q-1)$ nicht erreichen kann. Hiernach wird sich das grösste, in der Summe

$$m_1 + m_2 + \ldots + m_{i-1}$$

enthaltene Vielfache von $q-1$ durch Hinzufügen von m_i um eine Einheit vermehren oder constant bleiben, jenachdem von den drei, oben unterschiedenen Fällen einer der beiden ersten oder der letzte stattfindet. Wenn man daher annimmt, dass

$$m_1 + m_2 + \ldots + m_\alpha = n_\alpha(q-1) + \mu_\alpha,$$

während $0 \leqq \mu_\alpha < q-1$ ist, so muss es genau n_α Mal geschehen, dass einer der beiden ersten Fälle eintritt.

Hiernach wird man bei Anwendung der angegebenen Transformationen des Factors $\psi(\mu_{i-1}, m_i)$

$$\Psi(\omega) = q^{n_\alpha} \cdot \frac{f(\omega)}{\varphi(\omega)} \tag{6}$$

finden, worin sowohl $f(\omega)$ als auch $\varphi(\omega)$ Producte aus solchen ψ-Functionen bedeuten, bei welchen die Argumente eine kleinere Summe geben als $q-1$.

3. Auf ψ-Functionen dieser Art lässt sich aber der Satz in Nr. 2 der 10. Vorlesung zur Anwendung bringen. Dabei unterscheiden wir wieder die drei früheren Fälle. Ist erstens $\mu_{i-1} + m_i = q-1$, so ist nach Gleichung (3):

$$\psi(\mu_{i-1}, m_i) = (-1)^{1+\mu_{i-1}} \cdot q = (-1)^{1+m_i} \cdot q;$$

in diesem Falle aber ist $\mu_i = 0$, und da man

$1.2.3.\ldots m_i = (q-1-\mu_{i-1})(q-2-\mu_{i-1})\ldots(q-m_i-\mu_{i-1})$

also

$(-1)^{m_i} . 1 . 2 . 3 \ldots . m_i \equiv (\mu_{i-1}+1)(\mu_{i-1}+2) \ldots . (\mu_{i-1}+m_i) \pmod{q}$,

folglich mit Rücksicht auf den Wilson'schen Satz

$$(-1)^{m_i} . \prod(m_i) . \prod(\mu_{i-1}) \equiv 1 . 2 . 3 \ldots . (\mu_{i-1}+m_i) \equiv -1 \pmod{q}$$

findet, so kann man schreiben, wenn man in üblicher Weise übereinkommt, unter $\Pi(0)$ die Einheit zu verstehen,

$$(7) \qquad (-1)^{1+m_i} \equiv \frac{\Pi(\mu_i)}{\Pi(\mu_{i-1}) . \Pi(m_i)} \pmod{q} .$$

Dass in dieser Congruenz ein Bruch auftritt, macht keine Schwierigkeit, da die Factoren des Nenners durch q nicht theilbar sind. Sooft nämlich A eine zu q relativ prime Zahl ist, kann man eine Zahl A' der Congruenz $AA' \equiv 1 \pmod{q}$ gemäss bestimmen, und unter dem Bruche $\frac{1}{A} \pmod{q}$ jede der Zahl $A' \pmod{q}$ congruente Zahl verstehen. In solcher Weise muss auch die vorige, sowie alle ähnlichen im Folgenden vorkommenden Congruenzen, welche Brüche enthalten, aufgefasst werden.

Ist zweitens $\mu_{i-1} + m_i > q - 1$, so wird nach dem Satze in Nr. 2 der 10. Vorlesung

$$\psi(q-1-\mu_{i-1}, q-1-m_i, \gamma) \equiv -\frac{\Pi(2q-2-\mu_{i-1}-m_i)}{\Pi(q-1-\mu_{i-1}) . \Pi(q-1-m_i)} \pmod{q}$$

sein. Da aber, wenn $k < q - 1$ ist,

$$1 . 2 . 3 \ldots . k \equiv (-1)^k . (q-1)(q-2) \ldots . (q-k)$$

$$\prod(q-1-k) . \prod(k) \equiv (-1)^k . 1 . 2 . 3 \ldots . (q-1) \equiv (-1)^{k+1} \pmod{q}$$

gefunden wird, so kann man auch schreiben:

$$\psi(q-1-\mu_{i-1}, q-1-m_i, \gamma) \equiv \frac{\Pi(\mu_{i-1}) . \Pi(m_i)}{\Pi(\mu_{i-1}+m_i-q+1)} \pmod{q}$$

oder auch, da in diesem Falle $\mu_{i-1} + m_i = q - 1 + \mu_i$ ist,

$$(8) \qquad \frac{1}{\psi(q-1-\mu_{i-1}, q-1-m_i, \gamma)} \equiv \frac{\Pi(\mu_i)}{\Pi(\mu_{i-1}) . \Pi(m_i)} \pmod{q}$$

wie in dem vorigen Falle.

Ist endlich drittens $\mu_{i-1} + m_i < q - 1$, so folgt nach demselben Satze

$$\psi(\mu_{i-1}, m_i, \gamma) \equiv -\frac{\Pi(\mu_{i-1}+m_i)}{\Pi(\mu_{i-1}) . \Pi(m_i)} \pmod{q}$$

oder, da jetzt $\mu_{i-1} + m_i = \mu_i$ ist,

$$(9) \qquad \psi(\mu_{i-1}, m_i, \gamma) \equiv -\frac{\Pi(\mu_i)}{\Pi(\mu_{i-1}) \cdot \Pi(m_i)} \pmod{q}.$$

Setzt man daher in die Functionen $f(\omega)$ und $\varphi(\omega)$ statt ω die primitive Wurzel γ, und nimmt auf die im Vorigen angegebene Bildungsweise derselben aus den ψ-Functionen, den drei unterschiedenen Fällen entsprechend, Rücksicht, so wird man mit Beachtung der Congruenzen (7), (8) und (9) offenbar die folgende Congruenz finden:

$$(10) \qquad \frac{f(\gamma)}{\varphi(\gamma)} \equiv (-1)^{\alpha-1-n_\alpha} \cdot \frac{\Pi(\mu_\alpha)}{\Pi(m_1)\Pi(m_2) \ldots \Pi(m_\alpha)} \pmod{q},$$

da der dritte Fall $\alpha - 1 - n_\alpha$ Mal eintreten wird.

4. Wir werden jetzt speciell von folgendem Producte handeln:

$$\prod_a (\omega^{-a\mu}, R),$$

in welchem a jeden der $\frac{p-1}{2}$ quadratischen Reste von p bezeichnen soll, welche kleiner als p sind, und die Multiplication sich über alle diese Zahlen zu erstrecken hat. Um den Werth dieses Products zu erhalten, muss man in der Gleichung (4) $\alpha = \frac{p-1}{2}$ und die Zahlen $m_1, m_2, \ldots . m_\alpha$ den verschiedenen Zahlen $a\mu$ gleich wählen. Wenn man nun aber in dem Ausdrucke

$$\psi(h, k) = \frac{(\omega^{-h}, R) \cdot (\omega^{-k}, R)}{(\omega^{-h-k}, R)}$$

für h, k Vielfache von μ, etwa $h = h'\mu$, $k = k'\mu$ setzt, und bezeichnet $\omega^{-\mu}$ mit r, sodass r eine primitive Wurzel der Gleichung $x^p = 1$ wird, so enthält der Ausdruck

$$\psi(h'\mu, k'\mu) = \frac{(r^{h'}, R) \cdot (r^{k'}, R)}{(r^{h'+k'}, R)}$$

nur noch die Wurzel r. Demnach wird auch in den beiden Functionen $f(\omega)$, $\varphi(\omega)$, welche sich in dem hier betrachteten Falle aus solchen ψ-Functionen zusammensetzen, nur r vorkommen können, deshalb sollen sie mit $f_a(r)$ und $\varphi_a(r)$, desgleichen $\Psi(\omega)$ durch $\Psi_a(r)$ bezeichnet werden. Wenn man ferner $\gamma^{-\mu} = u$ setzt, so werden die Functionen $f(\gamma)$, $\varphi(\gamma)$ in der Congruenz (10) durch $f_a(u)$, $\varphi_a(u)$ resp. zu ersetzen sein. Endlich wollen wir

bemerken, dass, wenn g irgend eine primitive Wurzel (mod. p) bedeutet, sämmtliche quadratische Reste von p den Potenzen $1, g^2, g^4, \ldots . g^{p-3}$ (mod. p) congruent sind, folglich wird die, auf alle oben definirten Zahlen a bezogene Summe

$$\sum_a a \equiv 1 + g^2 + g^4 + \ldots . + g^{p-3} \pmod{p}$$

d. h. congruent Null sein; Σa ist also eine durch p theilbare, desgleichen also auch $\sum_a a\mu$ eine durch $p\mu = q - 1$ theilbare ganze Zahl. Hiernach wird $\mu_\alpha = 0$, $n_\alpha = \frac{\sum_a a\mu}{q-1} = \frac{\Sigma a}{p}$ sein, und die Formeln (6) und (10) gehen in die folgenden über:

$$(11) \qquad \Psi_a(r) = q^{\frac{\Sigma a}{p}} \cdot \frac{f_a(r)}{\varphi_a(r)}$$

$$(12) \qquad \frac{f_a(u)}{\varphi_a(u)} \equiv -(-1)^{\frac{p-1}{2} - \frac{\Sigma a}{p}} \frac{1}{\prod_a (1 \cdot 2 \cdot 3 \ldots . \mu a)} \pmod{q};$$

in dem Producte der letzten Formel muss wieder über alle oben definirten Zahlen a multiplicirt werden.

Bezeichnen wir ebenso mit b alle quadratischen Nichtreste von p, welche kleiner sind als p, und bilden das Product

$$\prod_b (\omega^{-b\mu}, R)$$

auf alle diese Werthe b bezogen, so gelten ganz dieselben Betrachtungen. Da

$$\sum b \equiv g + g^3 + g^5 + \ldots . + g^{p-2} \pmod{p}$$

also durch p theilbar ist, so ergiebt sich wieder $\mu_\alpha = 0, n_\alpha = \frac{\Sigma b}{p}$; bezeichnet man ferner mit $\Psi_b(r)$, $f_b(r)$, $\varphi_b(r)$ die auf diesen Fall bezüglichen Werthe der Functionen $\Psi(\omega)$, $f(\omega)$, $\varphi(\omega)$, so ergeben sich aus den Formeln (6) und (10) die nachstehenden:

$$(13) \qquad \Psi_b(r) = q^{\frac{\Sigma b}{p}} \cdot \frac{f_b(r)}{\varphi_b(r)}$$

$$(14) \qquad \frac{f_b(u)}{\varphi_b(u)} \equiv -(-1)^{\frac{p-1}{2} - \frac{\Sigma b}{p}} \cdot \frac{1}{\prod_b (1 \cdot 2 \cdot 3 \ldots . \mu b)} \pmod{q}.$$

5. Andererseits geht aus der Gleichung (4), wenn man

$\alpha = \frac{p-1}{2}$ und die Zahlen $m_1, m_2, \ldots . m_\alpha$ den Zahlen $a\mu$ gleich setzt, deren Summe als eine durch $q - 1$ theilbare Zahl soeben nachgewiesen worden ist, folgende Gleichung

$$(15) \qquad \Psi_a(r) = -\prod_a (\omega^{-a\mu}, R) = -\prod_a (r^a, R)$$

hervor, da

$$(\omega^{-(m_1+m_2+\ldots+m_\alpha)}, R) = (\omega^{-\Sigma a\mu}, R) = -1$$

wird. Diese Gleichung lehrt aber, dass das Product eine, von R ganz unabhängige, nur aus r gebildete, ganze Function ist, deren Coëfficienten ganze Zahlen sein müssen, da die Coëfficienten in den einzelnen Factoren (r^a, R) solche Zahlen sind; es ist, mit andern Worten, eine, aus r zusammengesetzte, complexe ganze Zahl. Indessen ist dasselbe offenbar unveränderlich, wenn r durch irgend eine Potenz $r^{a'}$ ersetzt wird, worin a' selbst ein quadratischer Rest (mod. p) ist; denn die $\frac{p-1}{2}$ Zahlen aa' sind, wie leicht zu sehen, unter einander (mod. p) incongruent und wieder quadratische Reste, folglich stimmen ihre kleinsten positiven Reste, von der Ordnung abgesehen, auf welche es in dem Producte nicht ankommt, mit den Zahlen a im Ganzen überein. Da nun a' stets einer geraden Potenz von g, etwa g^{2h} (mod. p) congruent ist, und $r^{g^{2h}}$ derselben zweigliedrigen Periode angehört, wie r selber, kommt das Gesagte nach Nr. 5 der 6. Vorlesung darauf hinaus, dass das Product nicht eine Function der einzelnen Wurzeln der Gleichung $x^p = 1$, sondern vielmehr eine Function ihrer beiden zweigliedrigen Perioden, welche η_0, η_1 genannt werden mögen, sein muss. Man kann daher setzen:

$$(16) \qquad \prod_a (\omega^{-a\mu}, R) = A_0\eta_0 + A_1\eta_1,$$

worin A_0, A_1 ganze Zahlen bedeuten.

Genau ebenso findet sich, wie auch einfach durch Vertauschung von $\omega^{-\mu} = r$ mit einer der Wurzeln $r^{g^{2h+1}}$ d. h., da g^{2h+1} irgend einem Nichtreste (mod. p) congruent ist, mit einer der Wurzeln r^b hervorgeht,

$$(17) \qquad \prod_b (\omega^{-b\mu}, R) = A_0\eta_1 + A_1\eta_0,$$

auch ist

$$\Psi_b(r) = -\prod_b (\omega^{-b\mu}, R) . \tag{18}$$

Wenn wir uns von nun an auf die Voraussetzung, dass p die Form $4n + 3$ habe, beschränken, so können wir die Gleichung (17) etwas anders schreiben; denn vermittelst der Bemerkung, dass dann -1 ein quadratischer Nichtrest von p ist, und dass folglich die Zahlen $-b$ allen quadratischen Resten (mod. p) congruent sind, nimmt sie offenbar folgende Gestalt an:

$$\prod_a (\omega^{a\mu}, R) = A_0\eta_1 + A_1\eta_0 .$$

Erinnern wir uns hier, dass nach Formel (29) der 8. Vorl.

$$(\omega^{a\mu}, R) . (\omega^{-a\mu}, R) = (-1)^{a\mu} . q$$

ist, dann werden wir durch Verbindung der vorigen Gleichung mit der Gleichung (16), wenn wir beachten, dass die Anzahl der Factoren in jedem der beiden Producte gleich $\frac{p-1}{2}$, sowie dass $\sum_a a\mu$ durch $q - 1$ theilbar, also eine gerade Zahl ist, zu der folgenden Gleichung:

$$q^{\frac{p-1}{2}} = (A_0\eta_0 + A_1\eta_1)(A_0\eta_1 + A_1\eta_0)$$

gelangen, welche, wenn für die Perioden ihre in Nr. 2 der 15. Vorlesung gefundenen Werthe

$$\eta_0 = \frac{-1+\sqrt{-p}}{2}, \quad \eta_1 = \frac{-1-\sqrt{-p}}{2}$$

substituirt werden, in die andere Gestalt:

$$4 . q^{\frac{p-1}{2}} = (A_0 + A_1)^2 + p(A_0 - A_1)^2 \tag{19}$$

übergeht.

6. Die so gewonnene Formel kann noch vereinfacht werden, wenn man sie durch die höchste Potenz von q, welche den Quadraten $(A_0 + A_1)^2$ und $(A_0 - A_1)^2$ gemeinsam sein kann, dividirt. Zur Bestimmung dieser Potenz dienen aber die Relationen (11) bis (14), von denen die erste und dritte, wenn angenommen wird, die höchste, den Zahlen A_0, A_1 gemeinsame, Potenz von q sei q^t,

mit Rücksicht auf (16) und (17) auch so geschrieben werden können:

$$(20)\quad \begin{cases} \frac{A_0}{q^t}\cdot\eta_0 + \frac{A_1}{q^t}\cdot\eta_1 = -\,q^{\frac{\Sigma a}{p}-t}\cdot\frac{f_a(r)}{\varphi_a(r)} \\ \frac{A_0}{q^t}\cdot\eta_1 + \frac{A_1}{q^t}\cdot\eta_0 = -\,q^{\frac{\Sigma b}{p}-t}\cdot\frac{f_b(r)}{\varphi_b(r)}\,. \end{cases}$$

Wir wollen nun zwischen den Wurzeln der Gleichung

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$$

und den Wurzeln der Congruenz

$$x^{p-1} + x^{p-2} + \ldots + x + 1 \equiv 0 \pmod{q}$$

genau dieselbe Correspondenz herstellen, wie in Nr. 2 der vor. Vorlesung, bei welcher u^h die zu r^h gehörige Congruenzwurzel war. Dann ist zunächst leicht nachzuweisen, dass keine der Zahlen $\frac{\Sigma a}{p}$, $\frac{\Sigma b}{p}$ kleiner als t sein kann; denn wäre z. B. $\frac{\Sigma a}{p} < t$, so entstünde aus der ersten der vorhergehenden Gleichungen die folgende:

$$q^{t-\frac{\Sigma a}{p}}\cdot\left(\frac{A_0}{q^t}\cdot\eta_0 + \frac{A_1}{q^t}\cdot\eta_1\right) = -\frac{f_a(r)}{\varphi_a(r)}\,,$$

und diese ginge nach dem Hauptsatze in Nr. 6 der 17. Vorlesung durch Substitution der Congruenzwurzeln statt der zugehörigen Gleichungswurzeln in die richtige Congruenz:

$$q^{t-\frac{\Sigma a}{p}}\cdot\left(\frac{A_0}{q^t}\cdot u_0 + \frac{A_1}{q^t}\cdot u_1\right) \equiv -\frac{f_a(u)}{\varphi_a(u)} \pmod{q},$$

in welcher

$$u_0 = u + u^{g^2} + \ldots + u^{g^{p-3}}$$

$$u_1 = u^g + u^{g^3} + \ldots + u^{g^{p-2}}$$

gesetzt ist, über und lieferte $\frac{f_a(u)}{\varphi_a(u)} \equiv 0 \pmod{q}$, was mit der Congruenz (12) unverträglich ist.

Wenn hierdurch nachgewiesen ist, dass die Zahlen $\frac{\Sigma a}{p}$, $\frac{\Sigma b}{p}$ mindestens gleich t sein müssen, so zeigen die Congruenzen:

$$(21)\qquad \left.\begin{aligned} \frac{A_0}{q^t}\cdot u_0 + \frac{A_1}{q^t}\cdot u_1 &\equiv -\,q^{\frac{\Sigma a}{p}-t}\cdot\frac{f_a(u)}{\varphi_a(u)} \\ \frac{A_0}{q^t}\cdot u_1 + \frac{A_1}{q^t}\cdot u_0 &\equiv -\,q^{\frac{\Sigma b}{p}-t}\cdot\frac{f_b(u)}{\varphi_b(u)} \end{aligned}\right\} (\text{mod. } q),$$

welche aus den Gleichungen (20) entstehen, indem die Gleichungswurzeln durch die zugehörigen Congruenzwurzeln ersetzt werden, dass nicht beide Zahlen grösser als t sein können. Denn sonst würde

$$(22)\quad \text{folglich}\qquad \left.\begin{aligned} A_0 u_0 + A_1 u_1 &\equiv 0,\ A_0 u_1 + A_1 u_0 \equiv 0 \\ A_0 (u_0^2 - u_1^2) &\equiv 0,\ A_1 (u_0^2 - u_1^2) \equiv 0 \end{aligned}\right\} (\text{mod. } q^{t+1}).$$

Es ist aber $u_0^2 - u_1^2 = (u_0 + u_1)\,(u_0 - u_1)$; von diesen Factoren ist der erste der negativen Einheit (mod. q) congruent, da

$$u_0 + u_1 = u + u^g + u^{g^2} + \ldots + u^{g^{p-2}} \equiv u + u^2 + \ldots + u^{p-1}$$

und

$$1 + u + u^2 + \ldots + u^{p-1} \equiv 0 \ (\text{mod. } q)$$

ist. Da ferner die Gleichung besteht

$$(\eta_0 - \eta_1)^2 = -\,p,$$

so erhält man die Congruenz

$$(u_0 - u_1)^2 \equiv -\,p \ (\text{mod. } q),$$

welche lehrt, dass auch der andere Factor, und folglich auch $u_0^2 - u_1^2$ nicht durch q theilbar ist. Demnach ergäbe sich aus den Congruenzen (22) das, der Bedeutung des Exponenten t widerstreitende Resultat, dass A_0 und A_1 durch q^{t+1} theilbar wären.

Aus diesen Betrachtungen ergiebt sich, dass, wenn nicht etwa $\frac{\Sigma a}{p}, \frac{\Sigma b}{p}$ gleichen Werth haben, t jedenfalls dem kleinern derselben gleich sein muss. Aber jene Voraussetzung ist unzulässig, da $\Sigma a + \Sigma b$ gleich der Summe

$$1 + 2 + 3 + \ldots + (p-1) = \frac{p\,(p-1)}{2}$$

in dem hier betrachteten Falle also, in welchem $\frac{p-1}{2}$ ungerade ist, einer ungeraden Zahl gleich ist, weshalb $\Sigma b - \Sigma a$ nicht gerade also auch nicht Null sein kann. Dasselbe folgt allgemein aus einem andern, bald zu erwähnenden Umstande, aus

welchem wir auch schliessen werden, dass Σb der grössere der beiden Werthe ist. Folglich muss $t = \frac{\Sigma a}{p}$ sein.

Wenn man nunmehr die Gleichung (19) mit dem Quadrate der grössten, den Zahlen A_0, A_1 oder den Zahlen $A_0 + A_1$, $A_0 - A_1$ gemeinsamen Potenz von q dividirt und

$$\frac{A_0 + A_1}{q^t} = x, \quad \frac{A_0 - A_1}{q^t} = y \tag{23}$$

setzt, sowie bemerkt, dass $\frac{\Sigma a}{p} + \frac{\Sigma b}{p} = \frac{p-1}{2}$ ist, so ergiebt sich endlich folgende höchst beachtenswerthe Gleichung:

$$4 \cdot q^{\frac{\Sigma b - \Sigma a}{p}} = x^2 + py^2, \tag{24}$$

welche den Satz enthält:

Ist p eine Primzahl von der Form $4n + 3$, q eine Primzahl von der Form $\mu p + 1$, und bezeichnen Σa, Σb die Summe resp. aller quadratischen Reste und Nichtreste (mod. p), welche kleiner als p sind, so gestattet das Vierfache der Potenz $q^{\frac{\Sigma b - \Sigma a}{p}}$ eine Darstellung durch die Form $x^2 + py^2$.

Die Congruenzen (21) können jetzt folgendermassen geschrieben werden, wenn auf (12) Rücksicht genommen wird:

$$\left.\begin{aligned} \frac{A_0}{q^t} \cdot u_0 + \frac{A_1}{q^t} \cdot u_1 &\equiv (-1)^{\frac{\Sigma b}{p}} \cdot \frac{1}{\prod_a (1 \cdot 2 \cdot 3 \ldots a\mu)} \\ \frac{A_0}{q^t} \cdot u_1 + \frac{A_1}{q^t} \cdot u_0 &\equiv 0 \end{aligned}\right\} \pmod{q}$$

und geben durch Addition die, zur Bestimmung von x dienende Congruenz

$$x \equiv -(-1)^{\frac{\Sigma b}{p}} \cdot \frac{1}{\prod_a (1 \cdot 2 \cdot 3 \ldots \mu a)} \pmod{q}. \tag{25}$$

So erhält man den Zusatz: Die Zahl x in der Darstellung (24) leistet der Congruenz (25) Genüge.

Noch kann beachtet werden, dass in dem Falle, wo p die Form $8n + 7$ hat, die Darstellung durch gerade Zahlen x, y geschieht; denn, wären sie, was sonst nothwendig wäre, da $x^2 + py^2$ gerade werden soll, Beide ungerade, so würden x^2, y^2 durch 8 getheilt den Rest 1 geben, $x^2 + py^2$ also durch 8 theil-

bar sein, während die andere Seite der Gleichung (24) es nur durch 4 ist. Setzt man daher $x = 2\xi$, $y = 2\eta$, so ergiebt sich der Folgesatz:

Ist p eine Primzahl von der Form $8n + 7$ und q eine Primzahl von der Form $\mu p + 1$, so giebt es ganze Zahlen ξ, η von der Beschaffenheit, dass

$$q^{\frac{\Sigma b - \Sigma a}{p}} = \xi^2 + p \cdot \eta^2$$

ist, während ξ der Congruenz

$$2\xi \equiv -(-1)^{\frac{\Sigma b}{p}} \frac{1}{\Pi(1 \cdot 2 \cdot 3 \ldots \mu a)} \pmod{q}$$

Genüge leistet.

Ist z. B. $q = 7\mu + 1$, so findet sich, da unter den Zahlen, welche kleiner als 7 sind, die Zahlen 1, 2, 4 die quadratischen Reste, die übrigen Zahlen 3, 5, 6 die quadratischen Nichtreste von 7 sind,

$$(26)\quad \begin{cases} q = \xi^2 + 7 \cdot \eta^2 \\ \text{wenn} \\ \xi \equiv -\frac{1}{2} \cdot \frac{1}{\Pi\mu \cdot \Pi 2\mu \cdot \Pi 4\mu} \pmod{q} \\ \text{ist, wofür man auch} \\ \xi \equiv \frac{1}{2} \cdot \frac{\Pi 3\mu}{\Pi\mu \cdot \Pi 2\mu} \pmod{q} \end{cases}$$

setzen kann, wenn man bemerkt, dass nach Wilson's Satze

$$-1 \equiv \prod 7\mu \equiv \prod 4\mu \cdot (4\mu + 1)(4\mu + 2) \ldots 7\mu$$
$$\equiv (-1)^{3\mu} \cdot 1 \cdot 2 \cdot 3 \ldots 3\mu \cdot \prod 4\mu \pmod{q}$$

ist, und μ nothwendig eine gerade Zahl sein muss. Dieses Resultat findet sich bereits in der in Nr. 3 der 11. Vorlesung citirten kleinen Abhandlung von Jacobi. —

Es ist zu beachten, dass die Zahlen ξ, η durch die Bedingungen (26) vollständig bestimmt sind, nämlich ξ als absolut kleinster Rest von q, welcher der Congruenz genügt, sodann η durch die quadratische Formel. Wenn jedoch in der Gleichung (24) eine höhere als die erste Potenz von q zur Linken des Gleichheitszeichens steht, wird die Darstellung durch die Bedingungen (24) und (25) im Allgemeinen noch nicht vollständig bestimmt sein. Während wir einige darauf bezügliche Einzelheiten hier übergehen wollen,

müssen wir noch auf den Zusammenhang, welcher zwischen diesen Betrachtungen und einer wichtigen Frage aus der Theorie der quadratischen Formen besteht, soweit es ohne näheres Eingehen auf diese Theorie möglich ist, hinweisen.

7. Man versteht in der Zahlentheorie unter einer (binären) quadratischen Form jeden Ausdruck von der folgenden Gestalt:

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

in welchem die Coëfficienten a, b, c ganze Zahlen sind; der Ausdruck $b^2 - ac$ heisst die Determinante der Form. Zwei solche Formen

$$ax^2 + 2bxy + cy^2,\ a'x'^2 + 2b'x'y' + c'y'^2$$

von gleicher Determinante werden äquivalent oder zu derselben Classe gehörig genannt, wenn die erste in die zweite mittelst einer linearen Transformation

$$x = \alpha x' + \beta y',\ y = \gamma x' + \delta y'$$

übergeführt werden kann, in welcher die Coëfficienten α, β, γ, δ ganze, der Gleichung $\alpha\delta - \beta\gamma = 1$ genügende Zahlen sind. Haben die Coëfficienten a, $2b$, c der Form keinen gemeinschaftlichen Theiler, so heisst sie eigentlich primitiv, wenn sie den grössten gemeinsamen Theiler Zwei haben, uneigentlich primitiv.

Denkt man sich nun alle uneigentlich primitiven Formen der Determinante $-p$, so zerfallen diese in eine gewisse, stets endliche Anzahl H verschiedener Classen von, unter einander äquivalenten, Formen. Die Bemerkung aber, welche wir hier anschliessen wollten, besteht darin, dass, wie Dirichlet auf höchst merkwürdige Weise, indem er die Analysis mit der Zahlentheorie in Verbindung brachte, nachgewiesen hat, die Zahl H genau gleich dem Exponenten von q in der Gleichung (24) nämlich

$$H = \frac{\Sigma b - \Sigma a}{p}$$

ist. Es ist hier nicht der Ort, auf Dirichlet's Methoden näher einzugehen, vielmehr muss auf seine betreffenden Arbeiten, deren wesentlichste in den Bänden 19, 21, 24 des Crelle'schen Journals enthalten sind, oder auch auf seine Vorlesungen über Zahlentheorie verwiesen werden. Nur das Eine muss zur Ergänzung des oben Gesagten hinzugefügt werden, dass aus dem Dirichlet-

schen Resultate unmittelbar die Beziehung $\Sigma b > \Sigma a$ hervorgeht, da die Anzahl H der Classen ihrer Natur nach stets eine positive ganze Zahl sein muss. Auf anderm Wege ist derselbe Umstand bisher nicht bewiesen worden, auch dürfte es, um mit Dirichlet zu reden*), nicht leicht sein, dafür einen arithmetischen Beweis zu finden.

Zum Schluss ist auf eine Notiz von Jacobi**) hinzuweisen, welche besonders geeignet ist, den Scharfsinn dieses grossen Mathematikers zu bezeugen. Die Theorie der quadratischen Formen lehrt, dass, wenn das Doppelte einer Primzahl q überhaupt durch uneigentlich primitive Formen der Determinante $-p$ darstellbar ist, es stets eine gewisse kleinste ganze Zahl h giebt von der Beschaffenheit, dass $2 \cdot q^h$ durch die sogenannte Hauptform

$$2x^2 + 2xy + \frac{p+1}{2} y^2$$

darstellbar ist; diese Zahl h muss stets gleich der Classenzahl H oder wenigstens ein Divisor derselben, und jede grössere Zahl derselben Beschaffenheit muss ein Vielfaches von der kleinsten Zahl h sein. Bemerken wir nun, dass die Zahlen x, y in der Gleichung (24) entweder Beide gerade, oder Beide ungerade sein müssen, damit die Summe $x^2 + py^2$ eine gerade Zahl wird, so ist klar, dass, wenn

$$x = 2X + Y, \; y = Y$$

gesetzt wird, für X, Y ganzzahlige Werthe sich ergeben werden. Durch diese Transformation geht aber die Form $x^2 + py^2$ in

$$2\left(2X^2 + 2XY + \frac{p+1}{2} Y^2\right)$$

über, und aus der Gleichung (24) ergiebt sich die folgende:

$$2 \cdot q^{\frac{\Sigma b - \Sigma a}{p}} = 2X^2 + 2XY + \frac{p+1}{2} Y^2.$$

Hieraus folgt nach dem eben Bemerkten jedenfalls, dass die Anzahl H der Classen uneigentlich primitiver Formen von der Determinante $-p$ mit der Zahl $\frac{\Sigma b - \Sigma a}{p}$ in einem einfachen Verhältnisse stehen wird. Da Jacobi aber bei einer Reihe von

*) s. Abhandl. d. Berl. Academie Jahrg. 1837 pag. 57.
**) in Crelle's J. Bd. 9 pag. 189.

Beispielen fand, dass H dieser Zahl selbst gleich wurde, sprach er den Satz aus, dass überhaupt die Classenanzahl H durch die Formel

$$H = \frac{\Sigma b - \Sigma a}{p}$$

bestimmt werde, ein Satz, der, wie schon gesagt wurde, durch Dirichlet's Forschungen eine glänzende Bestätigung gefunden hat.

8. Doch wir wenden uns nunmehr zu der letzten Anwendung, welche wir von der Kreistheilung machen wollen; sie betrifft einen, für die Theorie der quadratischen Formen von positiver Determinante wichtigen Gegenstand. Wenn wir uns auch hier auf den einfachsten Fall beschränken, in welchem die Determinante eine positive Primzahl p ist, so spielt in der Theorie der Formen von solcher Determinante die Aufgabe, alle ganzzahligen Lösungen t, u der sogenannten Pell'schen Gleichung

$$t^2 - pu^2 = 1$$

zu finden, eine grosse Rolle. Da man indessen aus einer Auflösung, bei welcher u von Null verschieden ist, leicht alle übrigen finden kann, kommt es wesentlich darauf an, eine solche zu finden, und es ist nun sehr merkwürdig, dass auch hierzu die Kreistheilung das Mittel darbietet und gerade diejenige Auflösung finden lehrt, welche wieder zur Anzahl der Classen äquivalenter Formen von der Determinante p eine unmittelbare Beziehung hat.

Um dahin zu gelangen, müssen wir von den Resultaten der Nr. 3 der 15. Vorlesung unsern Ausgang nehmen. Wir haben dort die Formel erhalten:

$$4 \cdot \frac{x^p - 1}{x - 1} = Y(x)^2 - (-1)^{\frac{p-1}{2}} \cdot pZ(x)^2 . \tag{27}$$

Unterscheiden wir nun von vornherein die beiden Fälle, in denen p die Form $4n + 1$ oder die Form $4n + 3$ hat.

In dem erstern erhalten wir aus (27) durch die Substitution $x = 1$ folgende Formel:

$$4p = y^2 - pz^2 \tag{28}$$

wenn mit y, z die reellen ganzen Zahlen bezeichnet werden, in welche die Functionen $Y(x)$, $Z(x)$ bei solcher Substitution übergehen, und welche Beide von Null verschieden sind, da weder $4p = y^2$, noch $4p = -pz^2$ sein kann. Die Gleichung (28) lehrt

ausserdem, dass y durch p theilbar ist; setzt man also $y = p.y_0$ und der Uebereinstimmung wegen $z = z_0$, so ergiebt sich nach Division mit p

$$z_0^2 - p y_0^2 = -4 . \tag{29}$$

Diese Gleichung kann man auch so schreiben:

$$(z_0 + y_0 \sqrt{p})(z_0 - y_0 \sqrt{p}) = -4,$$

und durch ihre Quadrirung findet man, wenn man

$$(z_0 + y_0 \sqrt{p})^2 = (z_0^2 + p y_0^2) + 2 z_0 y_0 \sqrt{p} = z_1 + y_1 \sqrt{p}$$

setzt,

$$(z_1 + y_1 \sqrt{p})(z_1 - y_1 \sqrt{p}) = 16 . \tag{30}$$

Die ganzen Zahlen

$$z_1 = z_0^2 + p y_0^2, \; y_1 = 2 z_0 y_0$$

sind jedenfalls durch Zwei theilbar, wie für y_1 von selbst klar ist und für z_1 sich daraus ergiebt, dass man wegen (29) auch

$$z_1 = -4 + 2 p y_0^2$$

schreiben kann. Sind aber y_0, z_0 schon gerade Zahlen, so werden z_1, y_1 sogar durch Vier theilbar sein, und man findet dann

$$\left(\frac{z_1}{4} + \frac{y_1}{4}\sqrt{p}\right)\left(\frac{z_1}{4} - \frac{y_1}{4}\sqrt{p}\right) = 1$$

d. h. $t = \frac{z_1}{4}$, $u = \frac{y_1}{4}$ ist eine ganzzahlige Auflösung der Pell'schen Gleichung

$$t^2 - p u^2 = 1$$

von der gesuchten Art, da y_0, z_0, y_1, u von Null verschieden sind. Dieser Fall tritt stets ein, wenn p die Form $8n + 1$ hat.

Wenn dagegen z_0, y_0 ungerade sind, was sie, damit $z_0^2 - p y_0^2$ gerade werde, gleichzeitig sein müssen, wenn sie nicht Beide gerade sind, so sind y_1, z_1 nur durch 2 theilbar, also z_2, y_2 ungerade, wenn man

$$z_1 = 2 z_2, \; y_1 = 2 y_2$$

setzt, und es ergiebt sich dann aus (30)

$$(z_2 + y_2 \sqrt{p})(z_2 - y_2 \sqrt{p}) = 4 .$$

Erhebt man diese Gleichung zum Cubus und setzt

$$(z_2 + y_2 \sqrt{p})^3 = (z_2^3 + 3 p z_2 y_2^2) + (3 z_2^2 y_2 + p y_2^3) \cdot \sqrt{p} = z_3 + y_3 \sqrt{p},$$

so übersieht man leicht, dass z_3, y_3 Beide durch 8 theilbar sind;

denn, da jetzt p die Form $8n + 5$ haben muss, so ergiebt sich

$$z_2^2 + 3py_2^2 \equiv 0,\ 3z_2^2 + py_2^2 \equiv 0 \pmod 8.$$

Da nun

$$(z_3 + y_3\sqrt{p})(z_3 - y_3\sqrt{p}) = 64$$

ist, findet man

$$\left(\frac{z_3}{8} + \frac{y_3}{8}\sqrt{p}\right)\left(\frac{z_3}{8} - \frac{y_3}{8}\sqrt{p}\right) = 1;$$

also sind die beiden ganzen Zahlen $t = \frac{z_3}{8}$, $u = \frac{y_3}{8}$ eine Lösung der Pell'schen Gleichung

$$t^2 - pu^2 = 1.$$

9. In dem zweiten Falle, wo p die Form $4n + 3$ hat, würde die Substitution $x = 1$ in der Gleichung (27) nur zu einer Identität führen. Wenn man dagegen $x = i$ setzt, so wird sich ein ähnliches Resultat ergeben, wie im vorigen Falle. Nach den Formeln (18) in Nr. 3 der 15. Vorlesung folgt bei dieser Substitution

$$Y(i) = -i^{\frac{p-1}{2}} \cdot Y(-i),\ Z(i) = i^{\frac{p-1}{2}} \cdot Z(-i).$$

Die Functionen $Y(i)$ und $Z(i)$ sind aber ganze complexe Zahlen von den Formen $y' + y''i$ und $z' + z''i$ resp. Wenn daher zunächst p die Form $8n + 3$ hat, so geben die vorigen Gleichungen folgende Beziehungen:

$$y' + y''i = -i(y' - y''i),\ z' + z''i = i(z' - z''i)$$

d. h.

$$y' = -y',\ z' = z'',$$

folglich werden $Y(i)$, $Z(i)$ von den Formen:

$$Y(i) = y'(1 - i),\ Z(i) = z'(1 + i).$$

Ist dagegen p von der Form $8n + 7$, so erhält man die Beziehungen:

$$y' + y''i = i(y' - y''i),\ z' + z''i = -i(z' - z''i),$$

aus denen $y' = y'',\ z' = -z''$ also

$$Y(i) = y'(1 + i),\ Z(i) = z'(1 - i)$$

hervorgeht.

Da andererseits $\frac{x^p - 1}{x - 1}$ für $x = i$ in $\frac{i^p - 1}{i - 1}$ übergeht, erhält es, wenn p die Form $4n + 3$ hat, den Werth i, und die

Gleichung (27) ergiebt demnach die nachstehende:

$$4i = y'^2 (1 \pm i)^2 + p z'^2 (1 \mp i)^2,$$

in welcher die doppelten Zeichen mit einander correspondiren, oder einfacher, da $(1 \pm i)^2 = \pm 2i$ ist,

$$y'^2 - p z'^2 = \pm 2, \tag{31}$$

was wir auch so schreiben können:

$$(y' + z' \sqrt{p})(y' - z' \sqrt{p}) = \pm 2 .$$

Erhebt man nun die letzte Gleichung in's Quadrat und setzt

$$(y' + z' \sqrt{p})^2 = y'^2 + p z'^2 + 2 y' z' \sqrt{p} = y'_1 + z'_1 \sqrt{p},$$

so sind

$$y_1' = y'^2 + p z'^2 = \pm 2 + 2 p z'^2, \; z_1' = 2 y' z'$$

gerade Zahlen, welche der Gleichung

$$(y_1' + z_1' \sqrt{p})(y_1' - z_1' \sqrt{p}) = 4$$

Genüge leisten, und $t = \frac{y_1'}{2}$, $u = \frac{z_1'}{2}$ zwei ganze Zahlen, für welche

$$(t + u \sqrt{p})(t - u \sqrt{p}) = 1$$

ist, d. h. eine ganzzahlige Lösung der Pell'schen Gleichung.

10. Hierdurch ist nachgewiesen, dass sich aus der Kreistheilung stets eine ganzzahlige Auflösung der Pell'schen Gleichung ableiten lässt. Diese ist jedoch nicht diejenige Auflösung, welche man als ihre Fundamentalauflösung zu bezeichnen pflegt, bei welcher nämlich die Zahlen t, u die kleinsten positiven Zahlen sind. Fragt man nun, in welcher Beziehung die so gefundenen Auflösungen zu der Fundamentalauflösung T, U stehen, so giebt die Antwort merkwürdiger Weise wieder einen innigen Zusammenhang zwischen der Kreistheilung und der Theorie der quadratischen Formen, insbesondere mit der Bestimmung der Classenanzahl zu erkennen. In der That, wenn wir uns der Kürze wegen auf den Fall einer positiven Determinante p von der Form $4n + 1$ beschränken, so folgt aus den von Dirichlet gefundenen Ausdrücken für die Anzahl H der Classen äquivalenter Formen von einer solchen Determinante folgende interessante Beziehung:

$$(T + U \sqrt{p})^H = \left(\frac{y + z \sqrt{p}}{y - z \sqrt{p}}\right)^{2 - \left(\frac{2}{p}\right)}, \tag{32}$$

wenn y, z die in Gleichung (28) vorkommenden ganzen Zahlen nämlich die Werthe $Y(1)$ und $Z(1)$ bedeuten, eine Beziehung, welche den Zusammenhang der, aus der Kreistheilung gewonnenen Auflösung mit der Fundamentalauflösung der Pell'schen Gleichung bezeichnet.

Dies Resultat giebt endlich noch zu einer Bemerkung Anlass, welche der über das Zeichen $\Sigma b - \Sigma a$ in Nr. 7 gemachten analog ist; die ganzen Zahlen y, z sind nämlich positiv. In der That, nach den Formeln in Nr. 3 der 15. Vorlesung ist

$$y+z\sqrt{p}=2A(1)=2\prod_a(1-r^a), y-z\sqrt{p}=2B(1)=2\prod_b(1-r^b).$$

Ist nun a ein quadratischer Rest, welcher grösser als $\frac{p}{2}$ ist, so wird, da -1 hier zu den quadratischen Resten gehört, $p-a$ ein quadratischer Rest sein, welcher $< \frac{p}{2}$ ist, und umgekehrt. Daraus folgt leicht, dass man, wenn a jetzt alle quadratischen Reste bezeichnet, welche $< \frac{p}{2}$ sind, setzen kann:

$$y + z\sqrt{p} = 2 \cdot \prod_a (1 - r^a)(1 - r^{-a})$$

oder, da $(1 - r^a)(1 - r^{-a}) = 2\left(1 - \cos\frac{2a\pi}{p}\right) = 4\sin^2\frac{2a\pi}{p}$, und die Anzahl der Werthe a gleich $\frac{p-1}{4}$ ist,

$$y + z\sqrt{p} = 2^{\frac{p+1}{2}} \cdot \left(\prod_a \sin\frac{2a\pi}{p}\right)^2.$$

Ganz ebenso findet man

$$y - z\sqrt{p} = 2^{\frac{p+1}{2}} \cdot \left(\prod_b \sin\frac{2b\pi}{p}\right)^2,$$

wenn man in dem Producte über alle quadratischen Nichtreste multiplicirt, die $< \frac{p}{2}$ sind. Diese Gleichungen lehren durch ihre Addition, dass y wesentlich positiv sein muss. Da aber T und U positiv sind, und

$$(T + U\sqrt{p})(T - U\sqrt{p}) = 1$$

ist, muss $T + U\sqrt{p} > 1$, folglich nach Gleichung (32)

$$\frac{y + z\sqrt{p}}{-z\sqrt{p}} > 1$$

sein, was nur geschehen kann, wenn auch z positiv ist. Auch diese Bemerkung ist bisher direct noch nicht bewiesen worden. —

Schliesslich mag erwähnt werden, dass, wenn man von den Darstellungen von $27X$ und $256X$ durch eine cubische resp. biquadratische Form ausgeht, welche durch die Gleichungen (40) der 15. und (39) der 16. Vorlesung gegeben werden, ähnliche Resultate, wie die hier aus der Darstellung von $4X$ durch eine quadratische Form abgeleiteten, gefunden werden können, wie es in Bezug auf die cubische Form in einer grossen Abhandlung von Eisenstein nachzulesen ist.*) Da es die Grenzen dieser Vorlesungen nicht gestatten, hierüber, noch auch über die wichtigen Forschungen Dirichlet's, die Classenanzahl betreffend, Ausführlicheres hier beizufügen, müssen wir den Leser, welcher darüber weiter unterrichtet zu sein wünscht, auf die bezüglichen Abhandlungen verweisen. —

*) Eisenstein, allgemeine Untersuchungen über die Formen 3^{ten} Grades mit drei Variabeln, welche der Kreistheilung ihre Entstehung verdanken, in Cr. J. Bd. 28.