Die Perioden der quadratischen Zahlformen bei negativen Determinanten.

Von **Wenzel Šimerka**,
Gymnasiallehrer zu Budweis.

(Vorgelegt in der Sitzung vom 14. Mai 1858.)

EINLEITUNG.

Die Periodicität der quadratischen Zahlformen, besonders jener der negativen Determinanten, hat sowohl ihre theoretische als auch praktische Seite. In ersterer Beziehung erscheinen alle Formen einer Determinante als ein regelmässiges leicht zu behandelndes Ganzes, man erlangt einen helleren Blick in die Reciprocität der Zahlen so wie in das eigenthümliche Gefüge der trinären Zahlformen und Zahlenwerthe. In letzterer Hinsicht liefert sie eine Regel dekadische Zahlen in Factoren zu zerlegen, die auch in Fällen anwendbar ist, wo keine der bisher bekannten Methoden ausreicht; überdies lassen sich mittelst derselben unbestimmte Gleichungen von der Gestalt $ax^2 + bxy + cy^2 = pz^m$ erschöpfend und bei grossen Determinanten lösen. Es kann daher die Wichtigkeit dieser Theorie nicht in Frage gestellt werden.

1. Zur Verwandlung und Gleichheit der quadratischen Zahlformen überhaupt.

Übergeht die Form $ax^2 + bxy + cy^2$, die man auch Kürze halber mit (a, b, c) bezeichnet, dadurch, dass $x = fx' + gy'$ und $y = mx' + ny'$ gesetzt wird, in $a'x'^2 + b'x'y' + c'y'^2 = (a', b', c')$, so wird, wenn beide Formen zu derselben Determinante gehören, gewöhnlich $fn - gm = \pm 1$ angenommen. Es geht jedoch, wie der weitere Verfolg dieser Abhandlung und besonders Nr. 16 zeigt, aus der Natur der quadratischen Zahlformen hervor, dass man die

Transformationsweise enger nehmen und blos $fn - gm = 1$ setzen dürfe.

Die nächste Folge hievon ist, dass $ax^2 + bxy + cy^2$ für $x = y'$ und $y = -x'$ in $cx'^2 - bx'y' + ay'^2$ übergehe, und man also $(a, b, c) = (c, -b, a)$ erhalte. Eine Form bleibt daher ungestört, wenn man ihre äusseren Coëfficienten versetzt, und zugleich das Zeichen des mittleren ins entgegengesetzte verwandelt.

Führt man diese Formen auf den einfachsten Ausdruck zurück, so wird entweder $x = x' + ky$ oder $y = kx + y'$ gesetzt; wesshalb dieses Verfahren auch bei obigem Grundsatze anwendbar ist.

Überdies erhellet, dass (a, b, c) mit $(a, -b, c)$ oder (c, b, a) im Allgemeinen nicht gleichgesetzt werden dürfe, weil man dann z. B. bei $x = x'$, $y = -y'$, $fn - gm = -1$ erhalten würde. Daraus geht auch hervor, dass das Vorzeichen des Mittelgliedes in diesen Formen eine ganz besondere Bedeutung habe.

2. Die Schluss- und Mittelformen.

Bei jeder Determinante D kommt wenigstens die Form $x^2 + Dy^2$, die man mit $(1, D)$ statt $(1, 0, D)$ bezeichnen kann, vor. Eben so hat jedes $D = 4d - 1$ die Form $x^2 + xy + dy^2 = (1, 1, d)$. Diese beiden Ausdrücke können rücksichtlich der weiter angeführten Gründe End- oder Schlussformen genannt werden.

Den Namen „Mittelformen“ kann man in Betracht des in der Folge ersichtlichen Baues der Perioden den Legendre'schen *diviseurs quadratiques bifides* beilegen. Diese Formen kommen bei den negativen Determinanten, wenn $D = pq$ ist, in den einfachsten Ausdrücken unter den Gestalten

$$\left(p,\ p,\ \frac{p+q}{4}\right)\ ,\ \left(\frac{p+q}{4},\ \frac{p-q}{2},\ \frac{p+q}{4}\right)$$

$$(p,\ q),\ \left(2p,\ 2p,\ \frac{p+q}{2}\right)\ ,\ \left(\frac{p+q}{2},\ p-q,\ \frac{p+q}{2}\right) \text{ vor,}$$

von denen die ersten zwei ein ungerades, die andern hingegen ein gerades Mittelglied besitzen. Nebst dem müssen alle drei Coëfficienten ganze Zahlen sein, und dürfen, wenn man diese Ausdrücke für Gauss'sche Formen der ersten Art ansieht, keinen gemeinsamen Theiler haben.

Dies vorausgeschickt gelangt man zu folgenden Sätzen:

a) Die obigen fünf Mittelformen reduciren sich auf drei, nämlich auf eine bei einem ungeraden, und auf zwei bei einem geraden Mittelgliede; denn wird in der ersten und vierten $y = -x + y'$ gesetzt, so übergehen sie in die zweite und fünfte. Es haben demnach die ungeraden Mittelformen nur die Gestalt (p, p, r), die geraden hingegen werden durch (p, q) und $(2p, 2p, r)$ repräsentirt. Auf diese Weise gelangt man zu der Form (a, ab, c), die als der allgemeine Ausdruck jeder Schluss- und Mittelform angesehen werden kann.

b) Das Vorzeichen des Mittelgliedes ist bei Schluss- und Mittelformen willkürlich, indem (a, ab, c) bei $x = x' - by$ in $(a, -ab, c)$ übergeht.

c) Die Mittelform $px^2 + pxy + \frac{p+q}{4} y^2$ erhält dadurch, dass man $x = x' + y'$ und $y = -2x' - y'$ setzt, die Gestalt $qx'^2 + qx'y' + \frac{p+q}{4} y'^2$.

Eben so findet man auch bei geraden Formen:

$$\left(2p, 2p, \frac{p+q}{2}\right) = \left(2q, 2q, \frac{p+q}{2}\right).$$

Jede Zerlegung von D in die Factoren p, q liefert daher nicht mehr als eine Mittelform der unter *a)* angeführten Gattungen.

d) Mittelformen von der Gestalt $\left(2p, 2p, \frac{p+q}{2}\right)$ kommen nur bei $D = 4\varphi + 1$ und 8φ vor. Ist nämlich im ersten Falle $p = 4\psi \pm 1$, so wird auch $q = 4\psi' \pm 1$ sein, und es erscheint als drittes Formglied $\frac{p+q}{2} = 2(\psi + \psi') \pm 1$ eine ganze und ungerade Zahl.

Ist, was den zweiten Fall anbelangt, $D = 2^\alpha mn$, wo $\alpha > 2$ und m, n ungerade Zahlen sind, so kann $p = 2m$, $q = 2^{\alpha-1} n$ genommen werden, und man gelangt zur Mittelform $(4m, 4m, m + 2^{\alpha-2} n)$, die nach *c)* auch die Gestalt $(2^\alpha n, 2^\alpha n, m + 2^{\alpha-2} n)$ bekommen kann.

e) Die Anzahl der ungeraden so wie der geraden Mittelformen bei Determinanten von der Gestalt $4\varphi + 2$, $4\varphi + 3$, $8\varphi + 4$

hängt blos von der Menge der Zerlegungen des D in die zwei Factoren p und q ab. Besteht daher D aus n relativen Primfactoren, so kann die Zerlegung bekanntlich auf eine 2^{n-1} fache Art vorgenommen werden. Jedes dieser Factorenpaare gibt eine Mittelform, nur $1 \times D$ liefert die Schlussform. Man erhält somit in diesem Falle $2^{n-1} - 1$ Mittelformen. So kommen bei $315 = 3^2 \times 5 \times 7$ wegen $n = 3$, drei, und bei $2100 = 2^2 \times 3 \times 5^2 \times 7$ sieben derartige Formen vor.

Was die Determinanten $D = 4\varphi + 1$ und 8φ anbelangt, so haben sie $2^{n-1} - 1$ Mittelformen von der Gestalt (p, q), da man hier ganz die obige Schlussweise anwenden kann. Überdies haben sie noch 2^{n-1} Formen von der Gestalt $\left(2p, 2p, \frac{p+q}{2}\right)$, indem jedes Factorenpaar ohne Ausnahme eine solche Form liefert. Daher haben diese Determinanten im Ganzen $2^n - 1$ Mittelformen. So kommen z. B. bei $105 = 3 \times 5 \times 7$ sieben, bei $840 = 2^3 \times 3 \times 5 \times 7$ aber 15 vor.

Hieraus folgt, dass die Primzahlen und Primpotenzen von der Gestalt $4\varphi + 1$ wegen $n = 1$ eine Mittelform haben, sie ist $(2, 2, 2\varphi + 1)$; eben so kommt bei $D = 2^m$ eine von der Gestalt $(4, 4, 2^{m-2} + 1)$ vor. Die übrigen Primzahlen und Primpotenzen haben keine Mittelformen.

3. Multiplication zweier quadratischen Zahlformen, deren ersten Coëfficienten prim zu einander sind.

Die Aufgabe, die unter dem obigen Namen verstanden wird, besteht darin, aus zwei Zahlformen derselben Determinante eine dritte von der Beschaffenheit zu finden, dass sie alle Producte von Zahlen der gegebenen Formen enthalte, überdies wie die beiden Factoren gerade oder ungerade sei, und ihrer Determinante angehöre. Hätte man vorerst die Formen $p = ax^2 + bxy + cy^2$ und $p' = a'x'^2 + b'x'y' + c'y'^2$, worin b, b' ungerade sind, so wird ihre Determinante

$$D = 4ac - b^2 = 4a'c' - b'^2 \tag{1}$$

sein.

Ferner erhält man:

$$4ap = (2ax + by)^2 + (4ac - b^2)\, y^2$$
$$4a'p' = (2a'x' + b'y')^2 + (4a'c' - b'^2)\, y'^2;$$

und wird in diesen Gleichungen

$$z = 2ax + by \qquad z' = 2a'x' + b'y' \tag{2}$$

gesetzt, so übergehen sie in:

$$4ap = z^2 + Dy^2 \quad , \quad 4a'p' = z'^2 + Dy'^2;$$

das Product hievon ist:

$$16aa'pp' = (zz' + i\, Dyy')^2 + D\,(zy' - i\, z'y)^2, \tag{3}$$

wo $i = \pm 1$ vorstellt, und im Verlaufe bestimmt wird. Ist nun

$$pp' = aa'\, X^2 + b''\, XY + c''\, Y^2 \tag{4}$$

eine den obigen Bedingungen genügende Form, so muss

$$D = 4aa'c'' - b''^2, \tag{5}$$

wesshalb b'' so zu bestimmen ist, dass $\frac{D + b''^2}{4a}$ und $\frac{D + b''^2}{4a'}$ ganze Zahlen werden. Dem wird mit Rücksicht auf die Gleichung 1) entsprochen, wenn

$$b'' = 2a\varphi + b = 2a'\varphi' + b' \tag{6}$$

genommen wird, mögen die Unbestimmten $\varphi\ \varphi'$ was immer für ganze Zahlen sein. Es würde wohl b'' die geforderten Bedingungen auch dann erfüllen, wenn etwa b' negativ genommen werden würde; dann wäre jedoch das Resultat ein Product der Formen $(a,\ b,\ c)$, $(a',\ -b',\ c')$; ist aber nach Nr. 1 das Vorzeichen des Mittelgliedes nicht gleichgiltig, so darf es auch hier nicht geändert werden. Was die Werthe von b'' anbelangt, so sind sie alle in $b'' = 2aa'\psi + \beta$ enthalten, wo $\beta \leqq aa'$, ψ jedoch beliebig ist; würde es nämlich noch eine Grösse β' von derselben Beschaffenheit wie β geben, so müsste $b'' \equiv \beta' \equiv \beta$ (Mod. a) und zugleich auch $b'' \equiv \beta' \equiv \beta$ (Mod. a') sein, d. h. $\beta' - \beta$ wäre durch aa' theilbar, was wegen $\beta' \leq aa'$ nur bei $\beta' = \beta$ stattfinden kann. Die Folge hievon ist, dass man für die Gl. 4 nur ein $b'' \leqq aa'$ findet, und dass daher durch die Multiplication

zweier Formen nur ein Resultat zum Vorschein kommt. Aus 4) und 5) folgt $16\,aa'pp' = (4aa'\,X + 2\,b''\,Y)^2 + D\,(2\,Y)^2$.

Wird diese Formel behufs der Auffindung von X, Y mit 3) gliederweise gleichgesetzt, so gelangt man zu

$$2\,Y = zy' - iz'y \quad ; \quad 4aa'\,X + 2b''\,Y = zz' + i\,Dyy'$$

oder nach 2)

$$Y = axy' - ia'x'y + \frac{b - ib'}{2}\,yy'$$

und $4aa'X = 4aa'xx' + 2a\,(b' - b'')\,xy' + 2a'\,(b + ib'')\,x'y$
$+ (bb' - bb'' + ib'b'' + iD)\,yy'$.

Da die Veränderlichen x, x', y, y' im Allgemeinen zu $4aa'$ prim sind, so müssen die Coëfficienten durch diese Grösse theilbar sein, und man findet nach 6)

$\frac{b' - b''}{2a'} = -\varphi'$, so wie auch $\frac{b + ib''}{2a} = i\varphi + \frac{b + ib}{2a}$, wesshalb $i = -1$ zu setzen ist, so dass $x'y$ zum Coëfficienten $-\varphi$ erhält. Beim letzten Theile ist mit Rücksicht auf 5)

$$\frac{1}{4aa'}\,(bb' - bb'' - b'b'' + b''^2 - 4aa'c'') =$$
$$\frac{(b'' - b)\,(b'' - b')}{4aa'} - c'' = \varphi\varphi' - c''.$$

Es ist demnach $X = xx' - \varphi' xy' - \varphi x'y + \varphi\varphi' yy' - c''yy'$ oder

$$X = (x - \varphi y)\,(x' - \varphi' y') - c''yy'$$

(7) und

$$Y = axy' + a'x'y + \tfrac{1}{2}\,(b + b')\,yy'.$$

Für c'' findet man noch den zur Rechnung bequemeren Ausdruck

(8) $$c'' = \frac{2c + (b + b'')\,\varphi}{2a'} \text{ oder } = \frac{2c' + (b' + b'')\,\varphi'}{2a}$$

Auf diese Weise gelangt man daher zu (a, b, c) $(a', b', c') = (aa', b'', c'')$.

Was die Formen mit geraden Mittelgliedern anbelangt, hat man nur statt b, b', b'', D beziehungsweise $2b$, $2b'$, $2b''$, $4D$ zu setzen, und erhält die Gleichung $b'' = a\varphi + b = a'\varphi' + b'$, woraus φ, φ', b'' gefunden wird, dann

$$c'' = \frac{c + (b + b'')\,\varphi}{a'} \text{ oder } = \frac{c' + (b' + b'')\,\varphi'}{a}$$

und $Y = a x y' + a' x' y + (b + b') y y'$. Der Werth von X ändert sich nicht.

1. Anmerkung. Wären a, a' nicht relative Primzahlen sondern etwa $a = \alpha h$, $a' = \alpha h'$, so fordert 6) dass $b \equiv b'$ (Mod. 2α) sei; im entgegengesetzten Falle müsste eine der Formen geändert werden. Da ferner nach 8) $b\varphi + c \equiv o$ und $b'\varphi' + c' \equiv o$ (Mod. α) ist, so findet man φ, φ' etwa in der Gestalt $\varphi = \alpha\psi + m$, $\varphi' = \alpha\psi' + m'$, dann übergeht 6) in $b'' = 2\alpha a\psi + 2am + b = 2\alpha a'\psi' + 2a'm' + b'$, woraus sich die Werthe von ψ, ψ' also auch φ, φ', b'', c'' ergeben.

   Dieses Verfahren findet jedoch wegen obiger Congruenzen bei geraden Formen, wenn a gerade ist, keine Anwendung.

2. Anmerkung. Weil $(a, b, c) = (c, -b, a)$ ist, so wird man auch $(a, b, c)^2 = (a, b, c)(c, -b, a)$ erhalten, und es reicht diese Methode zum Quadriren der Formen aus.

3. Anmerkung. Schon Lagrange und Legendre multiplicirten diese Zahlformen auf eine ähnliche Weise; sie erhielten aber aus jeder Multiplication zweier Formen zwei verschiedene Resultate, eines bei $+b$, $+b'$, das andere für $+b$ und $-b'$. Das vorstehende Verfahren verdient daher diesen Namen um so mehr, als hier wie überall die Factoren nur ein Product liefern, und beide zur Bildung desselben auf gleiche Weise beitragen, wie dies aus den Werthen von b'', c'', X und Y hervorgeht. Legendre ahnte zwar, wie Nr. 364 und 365 seines Werkes: *Essai sur la theorie des nombres (Edit. sec. 1818)* zeigt, die Periodicität dieser Formen, konnte sie jedoch aus obigem Grunde nicht finden.

4. Folgesätze.

Aus dem vorigen Abschnitte geht zunächst Nachstehendes hervor:

a) Es können auch mehr als zwei Formen mit einander multiplicirt werden. Hätte man etwa $p = (a, b, c)$, $p' = (a', b', c')$ $p'' = (\alpha, \beta, \gamma)$, so ist analog Nr. 3

$$b'' = 2a\varphi + b = 2a'\varphi' + b' = 2\alpha\varphi'' + \beta$$

dann

$$c'' = \frac{D + b''^2}{4\,a a' a} \text{ und } p\,p'\,p'' = (a a' a,\ b'',\ c'').$$

Daraus ergibt sich leicht das Verfahren bei geraden Formen und bei mehr als drei Factoren.

b) Wie man bei $D = 4\,a a' a c - \beta^2$, wenn a, a', a prim zu einander sind, aus den Formen

$$(a, \beta, a' a c)\ (a', \beta, a a c)\ (a, \beta, a a' c)$$

wegen $\varphi = \varphi' = \varphi'' = o$ das Product $(a a' a, \beta, c)$ erhält, so lässt sich wieder umgekehrt jede Form, deren erster Coëfficient ein Product ist, in ihre relativen Primfactoren zerlegen.

c) Die obige Multiplicationsregel gibt:

$$(a x^2 + b x y + c y^2)\,(c y'^2 + b x' y' + a x'^2) = a c\,X^2 + b X Y + Y^2,$$

wobei $X = x y' - x' y$ und $Y = a x x' + c y y' + b x' y$ ist.

Da man nun $(c, b, a) = (a, -b, c)$ hat, so liefern die Formen (a, b, c), $(a, -b, c)$ die Schlussform zum Producte. Aus diesem und aus mehreren der folgenden Sätze wird es klar, dass sich die Formen (a, b, c) und $(a, -b, c)$ wie entgegengesetzte Grössen zu einander verhalten.

d) Für Schluss- und Mittelformen hat man nach Nr. 2 den allgemeinen Ausdruck

$$p = a x^2 + a b x y + c y^2$$

oder $p = c x'^2 + a b x'\,(x + b y) + a\,(x + b y)^2$, wo $x' = -y$.

Das Product dieser beiden Formeln ist

$$p^2 = a c\,S^2 + a b\,S\,U + U^2 \text{ bei } S = -2 x y - b y^2$$

$$U = a x^2 + 2 a b x y + (a b^2 - c)\,y^2.$$

Wird hier $S = -Y$, $U = X + \mu Y$ gesetzt, indem man μ aus $a b - 2\mu = -1$ oder 0 bestimmt, so erscheint das Resultat unter der Gestalt

$$p^2 = X^2 + (2\mu - a b)\,X Y + (a c + \mu^2 - a b \mu)\,Y^2$$

bei $X = a x^2 + 2\,(a b - \mu)\,x y + (a b^2 - c - b \mu)\,y^2$ und $Y = 2 x y + b y^2$.

Demnach ist die Schlussform als das Quadrat ihrer selbst so wie auch jeder ihrer Mittelformen anzusehen.

In besonderen Fällen hat man:

1. bei $p = ax^2 + cy^2$, $P^2 = X^2 + acY^2$
und $X = ax^2 - cy^2$, $Y = 2xy$;

2. für $p = 2ax^2 + 2axy + cy^2$, $P^2 = X^2 + DY^2$,
$X = 2ax^2 + 2axy + (a - c)y^2$, $Y = 2xy + y^2$;

3. $p = ax^2 + axy + cy^2$, $P^2 = X^2 + XY + \frac{D+1}{4} Y^2$

und $X = ax^2 + (a-1)xy + \frac{a-1-2c}{2} y^2$,

$$Y = 2xy + y^2.$$

Für Schlussformen ist in 1) und 3) $a = 1$ zu nehmen.

c) Jeder Schlussform kann man in Berücksichtigung einer andern Form $ax^2 + bxy + cy^2$ die Gestalt $x'^2 + bx'y' + acy'^2$ geben, dann ist das Product dieser beiden Ausdrücke

$$aX^2 + bXY + cY^2,$$

wobei $X = xx' - cyy'$
und $Y = axy' + x'y + byy'$ bedeutet.

Daher gibt jede Form mit der Schlussform multiplicirt sich selbst zum Producte.

Dem zu Folge ist eine unpaare Potenz einer Mittelform wieder dieselbe Mittelform.

5. Multiplication der Formen mit Potenzen.

Vom Potenziren der Formen handelt Legendre in Nr. 362 etc.; dem vorgesetzten Ziele entspricht jedoch besser folgendes Verfahren: Hätte man bei der Determinante D die zwei Formen

$$p = a^m x^2 + bxy + cy^2, \quad p' = a^n x'^2 + b'x'y' + c'y'^2,$$

wo a zu D prim, und $b \equiv b'$ (Mod. $2a$) ist, so fordert ein ungerades b die Gleichung

$$D = 4a^m c - b^2 = 4a^n c' - b'^2 \qquad (1)$$

aus welcher wieder $n < m$ genommen

$$b^2 - b'^2 = (b + b')(b - b') = 4a^n (a^{m-n} c - c')$$

hervorgeht.

Ist daher a ungerade, so muss a^n in $b - b'$ aufgehen; würde nämlich für einen Theiler von a die Congruenz $b + b' \equiv o$ (Mod. a') bestehen, so hätte man wegen $b \equiv b'$ (Mod. a') auch $b \equiv b' \equiv 0$, und D hätte mit a den Divisor a' gemein. Wäre a gerade, so ist wegen $b \equiv b' \equiv \pm 1$ (Mod. 4), $b + b'$ eine Zahl von der Gestalt $2(2\mu + 1)$, und es kann, falls $a = 2^\alpha a'$ gesetzt wird, das ungerade a' aus obigem Grunde mit $b + b'$ keinen Theiler gemein haben; desshalb wird in

$$2(2\mu + 1)(b - b') = 4a^n (a^{m-n} c - c')$$

nur $a^{m-n} c - c'$ durch $2\mu + 1$ theilbar sein können, und es ist auch beim geraden a

$$b - b' = 2a^n w. \tag{2}$$

Dies vorausgeschickt erhält man aus den zwei gegebenen Formen

$$4a^m p = (2a^m x + by)^2 + Dy^2$$

und

$$4a^n p' = (2a^n x' + b'y')^2 + Dy'^2$$

und wird auch hier wie in Nr. 3

$$z = 2a^m x + by \qquad z' = 2a^n x' + b'y' \tag{3}$$

gesetzt, so gibt das Product dieser Gleichungen

$$16\, a^{m+n} pp' = (zz' - Dyy')^2 + D(zy' + z'y)^2. \tag{4}$$

Wäre die gesuchte Form

$$pp' = a^{m+n} X^2 + b'' XY + c'' Y^2, \tag{5}$$

wo vorerst aus der unbestimmten Gleichung

$$b\varphi + c = a^n \psi \tag{6}$$

die Werthe von φ, ψ bestimmt werden, die dann

$$b'' = 2a^m \varphi + b, \quad c'' = a^{m-n} \varphi^2 + \psi \tag{7}$$

liefern, so gehört die Form 5) zur Determinante D; denn es ist

$$\begin{aligned} 4a^{m+n}c'' - b''^2 &= 4a^m . a^n \psi - 4a^m b\varphi - b^2 = \\ &= 4a^m(b\varphi + c) - 4a^m b\varphi - b^2 \\ &= 4a^m c - b^2 = D. \end{aligned}$$

Hierauf gibt die Gl. 5)

$$16a^{m+n}pp' = (4a^{m+n}X + 2b''Y)^2 + D(2Y)^2$$

dies mit 4) gliederweise verglichen gibt vorerst

$$2Y = zy' + z'y$$

oder
$$Y = a^m xy' + a^n x'y + \tfrac{1}{2}(b + b')yy'. \tag{8}$$

Ferner ist

$$4a^{m+n}X + 2b''Y = zz' - Dyy',$$

welcher Ausdruck den Gl. 3) und 8) zufolge in

$$\begin{aligned} 4a^{m+n}X = 4a^{m+n}xx' - 2a^m(b'' - b')xy' - 2a^n(b'' - b)x'y \\ + (-bb'' - b'b'' + bb' - D)yy' \end{aligned}$$

übergeht.

Aus der Summe der Gl. 2) und 7) findet man

$$b'' - b' = 2a^m\varphi + 2a^n w = 2a^n\varphi';$$

überdies gibt die Gl. 7) $b'' - b = 2a^m\varphi$. Was den Coëfficienten von yy' anbelangt, hat man

$$\begin{aligned} (-bb'' - b'b'' + bb' + b''^2 - 4a^{m+n}c'') &= (b'' - b)(b'' - b') \\ - 4a^{m+n}c'' &= 4a^{m+n}\varphi\varphi' - 4a^{m+n}c''. \end{aligned}$$

Es ist also

$$X = xx' - \varphi' xy' - \varphi x'y + \varphi\varphi' yy' - c''yy'$$

oder
$$X = (x - \varphi y)(x' - \varphi' y') - c''yy', \tag{9}$$

wobei
$$\varphi' = \frac{b'' - b'}{2a^n} \text{ bedeutet.}$$

Was die Formen mit einem geraden Mittelgliede betrifft, so ist dieses Verfahren nach Gl. 6) nur für ein ungerades a brauchbar;

des entgegengesetzten Falles wird im folgenden Abschnitte erwähnt werden. Dann hat man

$$(a^m, 2b, c)\,(a^n, 2b', c') = a^{m+n}X^2 + 2b''XY + c''Y^2,$$

wo vorerst φ, ψ aus $2b\varphi + c = a^n\psi$ gesucht wird, wornach man

$$b'' = a^m\varphi + b,\quad c'' = a^{m-n}\varphi^2 + \psi,\quad \varphi' = \frac{b'' - b'}{a^n}$$

$$X = (x - \varphi y)\,(x' - \varphi' y') - c'' y y'$$

und

$$Y = a^m x y' + a^n x' y + (b + b')\,y y'$$

erhält.

Anmerkung. Viel kürzer ist die Multiplication von (a^m, b, c) (a^n, b', c') wenn $b \equiv -b'$ (Mod. $2a$). Aus dem eben Bewiesenen geht nämlich hervor, dass

$$(a^{m-n}, b, a^n c)\,(a^n, b, a^{m-n}c) = (a^m, b, c);$$

überdies folgt aus der Annahme von

$$b \equiv -b' \text{ (Mod. } 2a),\ (a^n, b, a^{m-n}c) = (a^n, -b', c'),$$

daher

$$(a^m, b, c)\,(a^n, b', c') = (a^{m-n}, b, a^n c)\,(a^n, -b', c')\,(a^n, b', c')$$

also nach Nr. 4 *pct. c* und $e = (a^{m-n}, b, a^n c)$.

Ist jedoch an den Werthen von X, Y gelegen, so muss die Operation nach schicklicher Veränderung der Formen auf eine andere Art vorgenommen werden.

6. Die Potenzen von 2 in geraden Formen.

Wenn man die Mittelformen $\left(2, 2, \frac{D+1}{2}\right)$ und $(2, d)$, deren Quadrate Schlussformen sind, übergeht, so ist es als Ergänzung des vorigen Abschnittes nöthig, hier zweier besonderer Fälle zu erwähnen, nämlich des Potenzirens von $(4, 2, 2k+1)$ bei $D = 8k + 3$, und der Multiplication von $(2^m, 2b, c)$, $(2^n, 2b', c')$.

a) Bei der Determinante $8k + 3$ kommen in ungeraden Formen nur ungerade Zahlen vor, und in den geraden Formen

erscheint von den Potenzen der Primzahl 2 blos 4 nämlich in

$$p = 4x^2 + 2xy + (2k+1)\,y^2.$$

Wollte man diese mit $p' = 4x'^2 + 2x'y' + (2k+1)\,y'^2$ multipliciren, so kann man zu den ungeraden Formen übergehen, dann ist nach dem vorigen Abschnitte wegen

$$a = a' = b = b' = m = n = 1,\ \varphi = -1,\ \psi = 2k,\ b'' = -1$$
$$c'' = 2k+1,\ \varphi' = -1,$$

daher $$pp' = X^2 - XY + (2k+1)\,Y^2;$$

aber $X = (2x+y)(2x'+y') - (2k+1)\,yy' = 2X'$

folglich ist das Product

$$pp' = 4X'^2 - 2X'Y + (2k+1)\,Y^2.$$

Dasselbe Resultat liefert Nr. 3, indem bei $(4,\ 2,\ 2k+1)$ $(2k+1, -2, 4)$ die Gleichung $b'' = 4\varphi + 1 = (2k+1)\,\varphi' - 1$ für $\varphi = k$, $\varphi' = 2$ lösbar ist; man erhält $b'' = 4k+1$, $c'' = 2k+1$ also $pp' = (8k+4)\,X^2 + (8k+2)\,XY + (2k+1)\,Y^2$, und wird hier $Y = Y' - 2X$ gesetzt, so kommt

$$pp' = 4X^2 - 2XY' + (2k+1)\,Y'^2$$

zum Vorschein.

Ist demnach $p = (4,\ 2,\ c)$, so hat man $p^2 = (4, -2, c)$, dann nach Nr. 4 $c\ p^3 = (1, D)$, $p^4 = (4, 2, c)$ u. s. w., d. h. p gibt eine Periode von 3 Gliedern.

b) Was den zweiten Fall anbelangt, so sind b, b', c, c' ungerade, und man findet unter den ungeraden Formen bei $D = 8k-1$ auch zwei von der Gestalt

$$p = 2^{m-2}x^2 + bxy + cy^2,\ p' = 2^{n-2}x'^2 + b'x'y' + c'y'^2,$$

aus denen die obigen für $x = 2t$, $x' = 2t'$ entstehen. Diese letzteren geben

$$pp' = 2^{m+n-4}X^2 + b''XY + c''Y^2.$$

Ist hier, wie vorausgesetzt wird, x zu y und x' zu y' prim, so werden p, p', Y ungerade, X hingegen $= 2X'$ sein, und es ist in geraden Formen

$$pp' = 2^{m+n-2}X'^2 + 2b''X'Y + c''Y^2.$$

Da nun die mit p, p' bezeichneten Formen dieselben Zahlen enthalten wie $(2^m, 2b, c)$ und $(2^n, 2b', c')$, so hat das Product dieser letzteren Formen einen um zwei kleineren Exponenten, als dies sonst bei ungeraden Formen geschehen würde. Übrigens kommt in diesen Ausdrücken keine niedrigere Potenz von 2 als 8 vor, und zur Brauchbarkeit des Verfahrens ist erforderlich, dass $2b \equiv 2b'$ (Mod. 8) stattfinde.

Anmerkung. Hieraus ist ersichtlich, dass man $(a^m, 2b, c)$ mit $(a^n, 2b', c')$, wenn a gerade und grösser als 2 ist, nicht direct multipliciren könne.

7. Die Quadratwurzel aus einer Schlussform ist entweder wieder die Schlussform oder eine Mittelform.

Dieser Satz ist die *propositio inversa* von Nr. 4 *d*, nämlich, dass nur Schluss- und Mittelformen zu Quadraten erhoben Schlussformen geben. Legendre beweist ihn für den speciellen Fall, dass D eine Primzahl ist; zum vorstehenden Zwecke ist jedoch ein allgemeiner Beweis erforderlich. Da ergeben sich zwei Hauptfälle, je nachdem man es mit ungeraden oder mit geraden Formen zu thun hat.

Erster Fall. Kommt p^2, wenn p eine ungerade D nicht theilende Primzahl ist, in einer ungeraden Schlussform vor, so hat man

$$p^2 = M^2 + MN + dN^2$$

und

$$D = 4d - 1.$$

Hieraus folgt

$$4p^2 = (2M + N)^2 + DN^2,$$

und wenn man

$$L = 2M + N$$

setzt,

$$4p^2 = L^2 + DN^2,$$

daher

$$DN^2 = (2p + L)(2p - L).$$

Ist nun $D = gh$, so wird man

$$2p + L = gA \text{ und } 2p - L = hB \qquad (1)$$

annehmen können, woraus dann $AB = N^2$ folgt. Dieser letzten Bedingung zufolge muss wieder $A = t^2E$, $B = u^2E$ gesetzt werden, so dass dann $N = tuE$ wird. Die Summe der Gleichungen unter 1) ist $4p = gA + hB$,

d. h. $$4p = E(gt^2 + hu^2). \qquad (2)$$

Hier kann nicht $E \equiv o \pmod{p}$ sein, weil Letzteres dann auch bei A, B, L, N und M der Fall wäre, oder mit anderen Worten, es müsste $M = p$ und $N = o$ sein, wo hier doch $N > o$ angesehen wird. Auch kann E nicht $= 2$ gesetzt werden; denn dann wäre $2p = gt^2 + hu^2$, wo wegen $gh = 4d - 1$, g und h ungerade sind. Wäre $t = 2t'$, so müsste auch $u = 2u'$ sein, und man hätte gegen die Voraussetzung $p = 2gt'^2 + 2hu'^2$.

Aber es kann auch nicht $t = 2t' + 1$ sein; denn dann wäre ebenfalls $u = 2u' + 1$, und man hätte

$$2p = 4(gt'^2 + gt' + hu'^2 + hu') + g + h.$$

Ist aber $g \equiv \pm 1 \pmod{4}$, so hat man $h \equiv \mp 1$, daher ist $g + h$ durch 4 theilbar, und p wäre wieder gerade. Es verbleiben also nur zwei Fälle:

a) $E = 1$ oder $4p = gt^2 + hu^2$. Da hier t mit u zugleich paar oder unpaar ist, so kann man $t = 2t' + u$ setzen und erhält

$$p = gt'^2 + gt'u + \frac{g+h}{4}u^2,$$

wo $$4g \times \frac{g+h}{4} - g^2 = D$$

ist. Für $g = 1$ gehört also p in die Schlussform, sonst aber in eine Mittelform. Oder es ist

b) $E = 4$, folglich $p = gt^2 + hu^2$. Setzt man $t = t' + u$, so wird $p = gt'^2 + 2gt'u + (g + h)u^2$, und übergeht man zu den ungeraden Formen durch die Annahme von $2u = u'$, so erhält man die Formel

$$p = gt'^2 + gt'u' + \frac{g+h}{4}u'^2,$$

worin von p das Vorhergesagte gilt.

Zweiter Fall. Ist die fragliche Schlussform eine gerade,

daher $$p^2 = M^2 + DN^2$$

oder $$DN^2 = (p + M)(p - M)$$

und $D = gh$, so kann nach der obigen Schlussweise

$$p + M = gA,\ p - M = hB$$

angenommen werden, woraus $N^2 = AB$ folgt, und man aus

$$A = t^2E,\ B = u^2E$$

(3) die Gleichung $$2p = E(gt^2 + hu^2)$$

erlangt. Für $E = 2$ kommt hier der obige Satz zum Vorschein. Ist jedoch $E = 1$ also $2p = gt^2 + hu^2$, so kann t mit u nicht zugleich gerade sein, und es sind nur die übrigen drei Fälle möglich:

Wäre $$t = 2t',\ u = 2u' + 1,$$

so muss $$h = 2h' \text{ und } p = 2gt'^2 + h'u^2$$

sein. Eben so findet man bei

$$t = 2t' + 1,\ u = 2u',\ g = 2g' \text{ und } p = g't^2 + 2hu'.$$

Sind jedoch t und u ungerade, so ist $t = 2t' + u$ anzunehmen erlaubt, und die Gleichung 3) übergeht in

$$p = 2gt'^2 + 2gt'u + \frac{g+h}{2}u^2.$$

In allen Fällen gehört also p zur Schluss- oder Mittelform.

8. Besondere Fälle des Potenzirens und Multiplicirens der Formen.

a) Werden in Nr. 5 die zwei Formen gleich gesetzt, so enthält das Product die Quadrate und Amben aller darin vorkommenden Primzahlen. Man erhält dann wegen

$$m = n = 1,\ b = b',\ c = c',\ x = x';\ y = y',\ p = p'$$

aus $$p = ax^2 + bxy + cy^2$$

die Gleichung $$b\varphi + c = a\psi$$

zu lösen,

wornach sich $b'' = 2a\varphi + b$, $c'' = \varphi^2 + \psi$, $\varphi' = \varphi$

ferner $X = x^2 - 2\varphi xy - \psi y^2$, $Y = 2axy + by^2$

und $p^2 = (a, b, c)^2 = a^2 X^2 + b'' XY + c'' Y^2$

ergibt. Eben so findet man die Quadrate der geraden Formen.

b) Vom Quadrate einer Form kann man successive zur dritten, vierten Potenz u. s. w. dadurch schreiten, dass man mit Beibehaltung des Resultates für die erste Form in der zweiten $n = 1$ setzt. Ist dann $p^m = (a^m, b, c)$ und $p = (a, b', c')$, so suche man φ, ψ aus $b\varphi + c = a\psi$, hierauf ist $b'' = 2a^m\varphi + b$, $c'' = a^{m-1}\varphi^2 + \psi$ und $p^{m+1} = (a^{m+1}, b'', c'')$. Diese Methode ist in vielen Fällen dem directen Potenziren der Formen (Legendre Nr. 362) vorzuziehen.

c) Nach Nr. 4 *b* hat man

$$(ah, bh, c) = (a, bh, ch)\ (h, bh, ac)$$

und eben so $(a'h, b'h, c') = (a', b'h, c'h)\ (h, b'h, a'c')$

Da ferner nach Nr. 2 *c* zu h, mag es paar oder unpaar sein, nur eine Mittelform gehört, deren Quadrat die Schlussform gibt, welche letztere die Formen nicht multiplicirt (Nr. 4 *e*), so gibt das Product obiger Gleichungen

$$(ah, bh, c)\ (a'h, b'h, c') = (a, bh, ch)\ (a', b'h, c'h),$$

welcher Satz oft in der Rechnung von bedeutendem Vortheil ist.

d) Sind M, M' zwei verschiedene Mittelformen derselben Determinante, so ist ihr Product M'' eine von ihnen beiden verschiedene Mittelform, und man findet überdies $MM' = M'$, $M'M' = M$. Es gibt nämlich die Gleichung $M \times M' = M''$ quadrirt $M^2 \times M'^2 = M''^2$, und bezeichnet man die Schlussform mit S, so erhält man $M''^2 = S$. Hier kann nicht $M'' = S$ sein; denn dann wäre $M \times M' = S$ also $M \times M'^2 = M' \times S = M'$, d. h. $M = M'$ gegen die Voraussetzung. Auch kann nicht $M'' = M$ oder $= M'$ sein, indem dann die andere Form $= S$ wäre. Es sind daher alle drei Mittelformen von einander verschieden.

Aus der Gleichung $M \times M' = M''$ folgt überdies

$$MM'' = M^2 \times M' = M'$$

und

$$M'M'' = M \times M'^2 = M$$

9. Bestimmbarkeit der Formen.

Bekanntlich sind Primzahlen und von ihren Potenzen alle jene, die zur Determinante prim sind, nur in einer quadratischen Form enthalten, mag nun D positiv oder negativ sein. Dieser Satz gibt ein Mittel an die Hand, wie man sich statt der Formen blosser Zahlen, welche jene Formen darstellen oder bestimmen, bedienen kann. In dieser Beziehung ist folgendes Verfahren das Zweckmässigste:

a) Kommt die Primzahl p in einer Form vor, so bringe man sie in's erste Glied derselben, wenn dies nicht schon der Fall ist, dass man (p, b, c) hat, wo b ohne Rücksicht auf das Vorzeichen $\leqq p$ gemacht werden kann. Da das Vorzeichen von b wichtig ist, so wird man am füglichsten diese Form nur dann $= p$ setzen können, wenn b positiv ist. Wäre z. B. $(9, 2, 34)$ durch eine Primzahl zu bestimmen, so kann man $x = x' - y$ nehmen, und erhält

$$(9, -16, 41) = (41, 16, 9) = 41 \text{ also } (9, 2, 34) = 41$$

b) Hieraus folgt, dass 1 die Bestimmungszahl der Schlussformen ist, was auch mit Nr. 4 d und e übereinstimmt. Eben so können auch die Mittelformen $\left(2, 2, \frac{D+1}{2}\right)$ oder $(2, d) = 2$ gesetzt werden.

c) Nach Nr. 4 c hat man $(a, b, c)\ (a, -b, c) = 1$ oder $(a, -b, c) = 1 : (a, b, c)$. Ist daher $P = (a, b, c)$, wo P was immer für eine Bestimmungszahl darstellt, so hat man

$$(a, -b, c) = 1 : P \text{ oder } \frac{1}{P}.$$

Es ist demnach $(p, -b, c) = \frac{1}{p}$, wenn b positiv und $< p$.

d) Was die Bestimmbarkeit der Form (p^m, b, c) anbelangt, hat man sich da, wie aus Nr. 5 erhellet, an den Rest, den b getheilt durch $2p$ gibt, zu halten; dieser wird immer zwischen den Grenzen $+p$ und $-p$ aufgesucht, ist er positiv, so hat man $(p^m, b, c) = p^m$

sonst aber $\frac{1}{p^m}$ oder p^{-m} zu setzen. Man wird daher z. B. $(8, 5, 9) = 2^3$ wegen $5 \equiv 1$ (Mod. 4), hingegen $(25, 16, 26) = \frac{1}{5^2}$ in Folge $16 \equiv -4$ (Mod. 10) anzunehmen haben.

e) Die Form $(aa'a''$ etc., b, $c)$ kann man sich nach Nr. 4 *b* in ihre Factoren $(a, b, a'a''c$ etc.), $(a', b, aa''c$ etc.), $(a'', b, aa'c$ etc.) zerlegt denken, wo a, a', a'' etc. Primzahlen oder Primpotenzen sind. Die Bestimmungsgrössen dieser Factoren werden aus den Resten, welche b getheilt durch die bezügliche doppelte Primzahl oder Wurzel gibt, ermittelt; ihr Product ist dann die Bestimmungszahl der gegebenen Form. Die Reste bei jenen Congruenzen müssen jedoch (nach *d*) immer kleiner sein, als die halben Divisoren. So ist z. B. $(180, -17, 193) = \frac{3^2 \times 5}{2^2}$ weil $180 = 2^2 \times 3^2 \times 5$ und $-17 \equiv -1$ (Mod. 4), $-17 \equiv 1$ (Mod. 6), $-17 \equiv 3$ (Mod. 10).

Anmerkung. Es ist als Nachtrag zu den Formenoperationen nicht zu überschen, dass eine Form durch eine andere dividirt wird, wenn man das Dividend mit dem negativen Divisor multiplicirt. Aus *c* folgt nämlich $(a, b, c) : (a', b', c') = (a, b, c), \times \frac{1}{(a', b', c')}$ $= (a, b, c)\,(a', -b', c')$. Auf dieselbe Weise wird auch eine Form aus einem Gliede einer Gleichung in das andere übertragen.

10. Existenz und Eigenschaften der Formen-Perioden.

a) Erhebt man $p = (a, b, c)$, wo p was immer für eine Bestimmungsgrösse vorstellt, zum Quadrat, dann zur dritten, vierten etc. Potenz, wobei man, um grossen Zahlen auszuweichen, die Formen reduciren und weiterhin blos mit (a, b, c) multipliciren kann, so enthalten die auf diese Art gefundenen Formen nach einander die Grössen p, p^2, p^3, p^4, . . . p^m . . . und man kann sie besserer Übersicht halber mit f_1, f_2, f_3, f_4 . . . . fm . . . . bezeichnen, wobei fm die m^{te} Form in der Verrechnung ist, und unter andern auch die m^{ten} Potenzen aller in der Basis (a, b, c) vorkommenden Primzahlen enthält. Die Grösse m kann der Zeiger oder Index heissen. Enthält

die Reihe $f_1, f_2, f_3 \ldots$ nur möglichst reducirte Ausdrücke, bei denen also der mittlere Coëfficient b keinen der äusseren übersteigt, so müssen sich dieselben einmal wiederholen, da nach diesem Verfahren jede Form eine neue liefert, folglich die Reihe nicht abbrechen kann, und eine Determinante nur eine endliche Anzahl Formen hat. Wiederholt sich nun eine Form, so wiederholen sich auch alle folgenden, da sie aus gleichen auf gleiche Weise entstehen, d. h. die Formen bilden eine Periode.

b) Es müssen sich aber auch, wenn $fm = fm'$ ist, alle vorhergehenden Formen wiederholen, denn weil man $fm = (a, b, c) f(m-1)$ hat, so wird $f(m-1) = (a, -b, c)\, fm$ und eben so auch $f(m'-1) = (a, -b, c)\, fm'$ gefunden. Daher entstehen alle vorhergehenden Glieder der Reihe aus den nachfolgenden nach demselben Gesetze, und die Periode hat sonach keine Vorglieder, weil auch das erste Glied $f1$ in der zweiten Periode vorkommen muss.

c) Ist θ die Anzahl der Periodenglieder oder kurz die Periodenlänge, so hat man $f(\theta+1) = f1 = (a, b, c)$ also nach Nr. 4 *c*

$$f\theta = (a, -b, c)\, f(\theta+1) = (a, -b, c)\,(a, b, c) = (1, b, ac),$$

und $f\theta$ ist die Schlussform, wodurch ihre Benennung gerechtfertigt wird.

d) Hat man $fm = (a', b', c')$, so ist auch $f(\theta - m) = p^{\theta-m} = p^{\theta} : p^m = 1 : fm = 1 : (a', b', c')$ oder $f(\theta - m) = (a', -b', c')$ d. h. je zwei Glieder einer Periode, deren Zeigersumme der Periodenlänge gleich ist, sind einander gleich aber entgegengesetzt. Jede Periode zerfällt daher, wie Ähnliches bei den periodischen Kettenbrüchen vorkommt, in zwei symmetrische Hälften.

e) Für die Verrechnung dieser Perioden sind folgende Sätze von Wichtigkeit:

$$fm \times fn = p^m \times p^n = p^{m+n} = f(m+n),$$

d. h. das Product zweier Formen hat zum Zeiger die Summe der Zeiger der Factoren. Ferner hat man $(fm)^n = (p^m)^n = p^{mn} = fmn$, und die Potenz einer Form hat zum Zeiger das Product aus dem Zeiger dieser Form und dem Exponenten.

Ist $fm = (a', b', c')$, so hat man auch

$$(a', -b', c') = \frac{1}{(a', b', c')} = \frac{1}{fm} = \frac{1}{p^m} = p^{-m} = f-m;$$

macht man daher das Mittelglied einer Form negativ, so mache man es auch mit ihrem Zeiger. Dass die negativen Zeiger jenen Gliedern zugehören, die vor $f1$, und $f0 = f\theta$ stehend gedacht werden, ist leicht einzusehen. Eben so ist aus dem Begriffe einer Periode klar, dass die Zeiger um jedes beliebige Vielfache von θ vermehrt oder vermindert werden können, und dass desshalb auch $m \equiv m'$ (Mod. θ) sein wird, wenn man $fm = fm'$ gefunden hat.

f) Ist θ eine ungerade Zahl, so hat die Periode zwei gleiche aber entgegengesetzte Formen zur Mitte nämlich $f\frac{1}{2}(\theta - 1)$ und $f\frac{1}{2}(\theta + 1)$; ist jedoch θ gerade, so befindet sich daselbst nur $f\frac{1}{2}\theta$, und weil $(f\frac{1}{2}\theta)^2 = f\theta = 1$ ist, so kann $f\frac{1}{2}\theta$ nur eine Mittelform sein, von welchem Umstande auch ihre Benennung entnommen ist.

Da die Primzahlen und Primpotenzen von der Gestalt $4d - 1$ keine Mittelformen haben (Nr. 2 *e*), so kann bei ihnen die Periodenlänge nur eine unpaare Zahl sein.

11. Versetzung der Periodenglieder. Einschliessende und eingeschlossene Perioden.

a) Wird nicht $f1$ sondern $f\alpha$ zur Basis der Periode genommen, so hat dann dieselbe zu Formenzeigern α, 2α, 3α, ... von denen diejenigen zu Schlussformen gehören, in denen θ aufgeht. Ist daher θ' die Länge der Periode, welche $f\alpha$ gibt, so muss $\frac{\alpha\theta'}{\theta}$ eine ganze Zahl sein. Ist also α zu θ prim, so hat man $\theta' = \theta$, und $f\alpha$ gibt dieselbe Periode wie $f1$, nur dass die Glieder in einer andern Ordnung vorkommen. Hieraus geht auch hervor, dass man die Zeiger mit jeder Zahl, die zu θ prim ist, multipliciren kann, um eine neue Anordnung der Periodenglieder zu erhalten. Wollte man daher $f\beta$, wo β zu θ prim ist, zur ersten in der Periode haben, und will die Zeiger der übrigen Formen kennen, so suche man aus der Congruenz $\beta\mu \equiv 1$ (Mod. θ) die Grösse μ, mit welcher die Zeiger der gegebenen Periode zu multipliciren sind. Oder sollte überhaupt $f\beta$ in $f'\gamma$ verwandelt werden, so wäre μ aus $\beta\mu \equiv \gamma$ zu suchen.

b) Sind α und θ nicht prim zu einander, so findet man θ' wegen $\frac{\alpha\theta'}{\theta}$ als den Nenner des so weit möglich gekürzten Bruches $\frac{\alpha}{\theta}$; daher ist θ' ein aliquoter Theil von θ. So hat die Periode, welche

$f1 = (5, 1, 504)$ bei $D = 10079$ gibt, 135 Glieder, darunter kommt auch $f60 = (3, 1, 840)$ vor. Die Periode, welche letztere Form liefert, hat daher wegen $\frac{60}{135} = \frac{4}{9}$ nur 9 Glieder.

Perioden, die in andern als ihre aliquoten Theile enthalten sind, können füglich eingeschlossene genannt werden, im entgegengesetzten Falle heissen sie einschliessend.

c) Gibt bei einer und derselben Determinante die Form p die Periode $f_1, f_2, f_3 \ldots f\theta$, dann die Form p' die Periode $f_1', f_2', f_3', \ldots f'\theta'$ und sind θ, θ' prim zu einander, so gibt $P = pp'$ zur Basis genommen eine Periode von $\theta\theta'$ Gliedern, welche die beiden obigen einschliesst.

Hier kann erstlich ausser der Schlussform keine andere in beiden Perioden zugleich enthalten sein; wäre dieses nämlich bei p'' der Fall, und gibt diese Form eine Periode von θ'' Gliedern, so müsste θ'' ein Theiler von θ und θ' sein, was nur bei $\theta'' = 1$ geschehen kann. Werden nun die Periodenglieder von P mit $F_1, F_2, F_3, \ldots$ bezeichnet, wo daher $F_1 = pp'$, $F_2 = p^2p'^2, \ldots$ ist, so ergibt sich zwischen den Formen dieser drei Perioden die Beziehung, dass man $Fu = fm \times f'n$ hat,

wenn $$u = \theta\varphi + m = \theta'\varphi' + n;$$

weil $$Fu = p^u p'^u = fu \times f'u = f(\theta\varphi + m) \times f'(\theta'\varphi' + n)$$
$$= fm \times f'n$$

wird. Ist ϑ die Periodenlänge von P, daher $F\vartheta = 1$, so muss, wenn $u = \vartheta$ gesetzt wird, m durch θ und n durch θ' theilbar sein; denn erhebt man $fm \times f'n = 1$ zur θ'^{ten} Potenz, so übergeht $fm\theta' \times f'n\theta' = 1$ wegen $f'n\theta' = 1$ in $fm\theta' = 1$, wesshalb man $m\theta' \equiv o$ (Mod. θ) oder $m \equiv o$ hat. Eben so findet man auch $n \equiv o$ (Mod. θ'). Folglich muss $\vartheta = \theta\theta'$ sein. Wird in obiger Gleichung $n = \theta'$ oder was dasselbe ist $= o$ gesetzt, so erhält man $Fu = fm$; daher schliesst die Periode von P jene, die p gibt, ein. Dasselbe ist mit p' der Fall, da man für $m = o$, $Fu = f'n$ erhält.

Dem zu Folge lassen sich zwei somit auch mehrere Perioden, deren Längen relative Primzahlen sind, in eine einzige verbinden, die sie alle einschliesst. Daher können Perioden von ungerader Gliederzahl bei Determinanten, welche Mittelformen haben, nur zu den eingeschlossenen gehören.

12. Die Periodensysteme.

Viele Determinanten haben ihre Formen in mehreren Perioden. Zu solchen gehören alle, die mehr als eine Mittelform besitzen, indem sie wenigstens so viele Perioden als Mittelformen haben müssen. Die zu einer Determinante gehörigen Perioden kann man füglich ihr Periodensystem nennen, welches sich, so weit ich bisher erforschen konnte, auf zwei Hauptfälle reduciren lässt, und zwar:

a) Kommen öfters k Perioden vor, deren Länge sämmtlich die Primzahl e ist, und bei denen kein Glied einer Periode aus den Gliedern der anderen Perioden entstanden ist. Diese k Perioden kann man nach §. 48 etc. der „combinatorischen Analysis vom Herrn Andreas von Ettingshausen“ als Variationsreihen, daher die einzelnen Formen als ihre Elemente ansehen, so dass dann das Product aus allen Elementen einer Variationsform eine quadratische Zahlform, die zu einer Periode von e Gliedern gehört, liefert, nur das Product der k Schlussformen gibt die allen Perioden gemeinschaftliche Schlussform. Auf diese Weise erhält man $e^k - 1$ Formen, die sämmtlich von einander verschieden sind. Heisst A die Anzahl der Perioden, so wird man $A = \frac{e^k - 1}{e - 1}$ haben, da zu jeder Periode $e - 1$ Formen gehören. Für $e = 2$ gibt z. B. A die Anzahl der Mittelformen $2^k - 1$ (vergl. Nr. 2). Oder $D = 307$ hat die Formen $(4, 2, 77)$, $(7, 2, 44)$, deren jede eine eigene dreigliedrige Periode gibt, daher hier $e = 3$, $k = 2$ folglich $A = 4$ ist. Dasselbe ist bei den geraden Formen von $D = 547$ der Fall.

Hat nun eine Determinante ausser jenen A Perioden noch eine θ gliedrige, wo e und θ prim zu einander sind, so entstehen aus ihrer Verbindung nach Nr. 11 A Perioden von der Länge $e\theta$, deren jede die obige θ gliedrige einschliesst; denn stellt $f_1, f_2, f_3, \ldots f^{\theta}$ die besagte Periode dar, und setzt man in der Gleichung

$$u = \theta\varphi + m = e\varphi' + n,\ u = eu',$$

daher $u = eu'$, so folgt aus $Fu = fm \times f^n$, mag f^n zu welcher der A Perioden immer gehören, $Feu' = fm$.

Daher kommen $f_1, f_2, f_3, \ldots$ an den durch e theilbaren Stellen aller $e\theta$ gliedrigen Perioden vor. So hat z. B. $D = 341$ drei

14 gliedrige Perioden, indem daselbst $e = 2$, $k = 2$, $\theta = 7$ ist; $D = 755$ hat die geraden Formen in vier 12gliedrigen Perioden, und $D = 2\,184499$ hat die ungeraden Formen wegen $e = 5, k = 2, \theta = 11$ in sechs 55 gliedrigen Perioden, was ein bedeutend seltener Fall ist.

b) Oft hat eine Determinante eine Periode von e^α Gliedern und über dies k von ihr und auch unter einander unabhängige e gliedrige Perioden, ist die erstere $f_1, f_2, f_3, \ldots . fe^\alpha$ und stellt $f''_1 f''_2 f''_3 \ldots f'e$ welche immer der aus jenen k entstandenen $\frac{e^k - 1}{e - 1}$ Perioden vor, so gehört $fm \times f'n$ einer e^α gliedrigen Periode an, wenn e in m nicht aufgeht; daher hat m so viele Werthe als e^α relative kleinere Primzahlen, d. i. $(e - 1)\, e^{\alpha-1}$, und da der Grösse n, e^k Werthe zukommen, so entstehen aus $fm \times f'n$ im Ganzen $(e - 1)\, e^{\alpha-1} \times e^k$ Formen, von denen je $(e - 1)\, e^{\alpha-1}$ zu einer e^α gliedrigen Periode gehören; daher ist die Anzahl dieser Perioden $= \frac{(e-1)\, e^{\alpha-1} \times e^k}{(e-1)\, e^{\alpha-1}} = e^k$.

Ist $F_1 = f_1 \times f'n$ das erste Glied welcher immer von diesen e^k Perioden, so hat man

$$(F1)^e = Fe = (f1)^e\,(f'n)^e = fe \times f'en = fe,$$

und eben so $F2e = f2e$, $F3e = f3e \ldots .$ d. h. alle diese Perioden haben die $e^{\alpha-1}$ gliedrige $fe, f2e, f3e, \ldots .$ gemeinschaftlich.

Ferner gibt $fem \times f'n$ bei der obigen Bedeutung von m eine $e^{\alpha-1}$ gliedrige Periode; m hat hier $(e - 1)\, e^{\alpha-2}$ Werthe, n jedoch nur $e^k - 1$, weil das Product der Schlussformen hier nicht zu berücksichtigen ist, indem dann $fem \times f'e$ Glieder der eingeschlossenen Periode geben würde. Es entstehen also auf diese Weise $(e - 1)\, e^{\alpha-2}\, (e^k - 1)$ Formen, deren zu einer Periode $(e - 1)\, e^{\alpha-2}$ gehören, folglich ist die Anzahl dieser $e^{\alpha-1}$ gliedrigen Perioden $= e^k - 1$.

Setzt man hier $F'1 = fe \times f'n$, so erhält man $F'ge = fge^2$, und eben so folgt aus $Fe = fe$, $Fge^2 = fge^2$; demnach schliessen beide Classen die Periode $fe^2, f2e^2, f3e^2, \ldots . fe^\alpha$ gemeinschaftlich ein, und man kann dieselben so ordnen, dass die Formen der ersten Classe, d. i. jene in e^α gliedrigen Perioden, deren Zeiger ge^2 sind, den Formen der zweiten Classe mit den Zeigern ge entsprechen.

Eben so gibt $fe^2m \times f'n$ eine dritte Classe von Perioden, deren Länge e^{a-2} und Anzahl $e^k - 1$ ist, und die sich zu jenen der zweiten Classe eben so verhalten, wie diese zu den Perioden der ersten Classe. Dasselbe gilt von den $e^{a-3}, e^{a-4} \ldots . e^2$ gliedrigen Perioden.

Zuletzt kommt man zu den e gliedrigen Perioden, deren Anzahl nach α) $\frac{e^{k+1}-1}{e-1} - 1 = e\frac{e^k-1}{e-1}$ beträgt, indem hier $k + 1$ ursprüngliche Perioden vorkommen, und $fe^{a-1}, f2e^{a-1}, \ldots . fe^a$ zu den eingeschlossenen gehört.

So findet man bei $D = 305$ zwei 8 gliedrige, eine 4 gliedrige und zwei 2 gliedrige Perioden, da $e = 2$, $a = 3$ und $k = 1$. Eben so hat $D = 1187$ drei 9 gliedrige und drei 3 gliedrige, weil $e = 3$, $a = 2$ und $k = 1$ ist.

Übrigens leuchtet ein, dass alle diese Perioden mit einer θ gliedrigen verbunden vorkommen können. So hat z. B. $D = 1517$ zwei 24 gliedrige, eine 12 gliedrige und zwei 6 gliedrige Perioden.

Anmerkung. Wollte man das Periodensystem übersichtlich darstellen, so könnten die Formen desselben mit f_n^m bezeichnet werden, welcher Ausdruck die n^{te} Form der m^{ten} Periode bedeuten würde; der Zusammenhang der einzelnen Perioden müsste dann eigends durch Gleichungen bestimmt werden. Dies scheint jedoch wenig Bedeutung zu haben.

13. Verrechnungsweise der Perioden.

Jede Periode kann als verrechnet angesehen werden, wenn man ihre Länge und eine hinreichende Anzahl ihrer wichtigeren Glieder kennt; denn dann lässt sich zu jedem Zeiger die Form und umgekehrt finden. Was die Länge θ anbelangt, sucht man $fm = 1$ zu erhalten, wo dann entweder $\theta = m$ oder ein Theiler von m ist. Die wichtigsten Glieder der Perioden sind die zu kleinen Primzahlen gehörigen Formen. Welches die grösste Primzahl wäre, deren Zeiger man kennen müsse, um vor Irrthum sicher zu sein, konnte ich bis jetzt nicht ermitteln, jedenfalls ist sie kleiner als $\sqrt{\frac{D}{3}}$ bei den unpaaren, und als $2\sqrt{\frac{D}{3}}$ bei den paaren Formen, wahrscheinlich aber reichen dazu nur wenige Primzahlen hin.

a) Bei mässigen Determinanten, wo man nur eine Periode vermuthet, kann die Verrechnung ohne weitere Hilfsmittel mittelst der Bestimmungsgrössen der Formen (Nr. 9) vorgenommen werden. Z. B. bei $D = 10079$ wäre $f1 = (5, 1, 504)$, $f2 = (25, 11, 102)$ $f3 = (36, 17, 72)$ also $f3 = \frac{2^2}{3^2}$ und zugleich $f3 = \frac{3^2}{2^3}$, folglich multiplicirt $f6 = \frac{1}{2}$ oder $f - 6 = 2$ und aus $2^3 f3 = 3^2$ wird $f - 15 = 3^2$. Ferner weil $f - 1 = 2^3 \times 3^2 \times 7$ ist, hat man $f32 = 7$ oder $(7, 1, 360)$ dies quadrirt $f64 = (49, -41, 60)$ und $f64 = \frac{2^2 \times 5}{3}$, woraus $f - 75 = 3$, also $f - 150 = f - 15 = 3^2$ oder $f135 = 1$ und $\theta = 135$ folgt, da θ weder 45 noch 27 etc. sein kann. Daraus ergibt sich dann $f129 = 2$, $f60 = 3$ u. s. w.

Lassen sich auf diese Art die Zeiger einiger Primzahlen nicht finden, so gibt die Basis entweder eine eingeschlossene Periode, oder es findet sich da ein Periodensystem vor. Im ersten Falle kann man eine andere Basis wählen oder die Perioden verschiedener Basen mit einander verbinden; im letzteren Falle ist ein anderes Verfahren einzuschlagen.

b) Bei grossen Determinanten, oder wo die vorige Methode nicht zum Ziele führt, nimmt man die Zeiger einiger kleiner Primzahlen als unbekannt an, scheidet dann jene Grössen aus den Producten der Bestimmungsgleichungen aus, und sucht die anderen Primzahlen in Bestimmungsgleichungen durch jene unbekannten Zeiger darzustellen. Findet man bei einer Grösse zwei verschiedene Zeiger, etwa $fm = fm' = p$, so hat man $m \equiv m'$ (Mod. θ), wo jedoch θ unbekannt ist. Aus mehreren solcher Ausdrücke, die man Periodengleichungen nennen kann, werden dann die unbekannten Zeiger und θ gefunden. Man braucht immer wenigstens so viele Periodengleichungen, als es Unbekannte gibt. Ein Beispiel mag dies erläutern:

Setzt man bei $D = 121271$, $fx = 2$, $fy = 3$, so folgt aus $f2.x = (4, -3, 7580) = (4, 5, 3 \times 7 \times 19^2)$, $f2.x = \frac{3}{7 \times 19^2}$, $7 \times 19^2 = \frac{fy}{f2.x}$, d. h. $f - 2.x + y = 7 \times 19^2$, dann gibt $f3.x = (8, 13, 3 \times 5 \times 11 \times 23)$, $f - 3.x - y = 5 \times 23 : 11$ und weiterhin ist $f4.x + 2y = 31 : 7$, $f - 5.x - y = 11 \times 29$

$f5x = 7 \times 29 : 5$, $f - 6x + 2y = 53$, $f - 6x - 3y = 5^2$ und aus $f7x$ geht $f15x = 1$ oder $15x \equiv o \pmod{\theta}$ hervor; nebst dem erhält man $f7x + y = 5 : 19$ und $f7x - y = 7 : 23$. Aus der Verbindung der ersten und vorletzten Gleichung folgt $f12x + 3y = 5^2 \times 7$ oder $f3x + 6y = 7$, $f - 4x + 7y = 23$ $f7x + 8y = 31$. Weiterhin gibt $f3y$, $f4y$, $f5y$, $f - x + 3y = 83 : 7$ oder $f2x + 9y = 83$, dann $fx + 4y = 11 \times 19$, $f3x - 5y = 7 \times 11$ also $f - 11y = 11$, $fx + 15y = 19$ daher $f8x + 16y = 5$, was mit dem Zeiger von 5^2 verglichen $22x + 35y \equiv o$ liefert. Multiplicirt man diese Gleichung mit 15, so ist wegen $22 \times 15x \equiv o$, $525y \equiv o$ und $\theta = 525y$. Ein Theiler von $525y$ kann θ nicht sein; wäre z. B. $\theta = 175y$, so folgt aus der fünffachen zweiten Periodengleichung $110x + 175y \equiv o$, d. h. $5x \equiv o$. Wird demnach $y = 1$ folglich $\theta = 525$ genommen, so gibt die Gleichung $22x + 35y \equiv o$, $x = 70$, woraus man $f51 = 5$, $f216 = 7$, $f515 = 11$ u. s. w. berechnet.

14. Die Periodengleichungen.

Von diesen gilt alles, was von Congruenzen überhaupt gilt, nur dürfen sie nicht, so lange der Modell unbekannt ist, dividirt werden, indem der Divisor leicht zum Modell nicht prim sein könnte. Auch ereignet es sich hier oft, dass sich eine der Gleichungen aus den anderen ableiten lässt, in welchem Falle dann a Gleichungen nicht hinreichen, um a unbekannte Zeiger zu bestimmen. Überdies haben sie folgendes Eigenthümliche:

a) Kommt unter ihnen eine von der Gestalt $2ax + 2by + 2cz \equiv o$ vor, oder lässt sich eine solche ableiten, so ist entweder $ax + by + cz \equiv o$ oder $\frac{1}{2}\theta$, und es gehört $f(ax + by + cz)$ einer Schluss- oder Mittelform an. Lässt sich diese Grösse aus den bekannten Periodengleichungen nicht ableiten, so ist das Letztere beinahe sicher, und hätte D schon die Mittelform $(2, 2, c)$ oder $(2, d)$, so wird der Zeiger $ax + by + cz$ wahrscheinlich einer andern Mittelform angehören. Dies ist besonders bei Factorenzerlegungen von Wichtigkeit.

b) Hat D zwei oder mehrere Gleichungen von der Gestalt $aex + bey + cez \equiv o$, $a'ex + b'ey + c'ez \equiv o$ oder lassen sich dieselben ableiten, zeigt es sich übrigens, dass keine von den

Grössen $ax + by + cz$, $a'x + b'y + c'z \equiv o$ ist, und dass sie sämmtlich von einander verschieden sind, so kommt bei D ein Periodensystem vor, das dann nach den Grundsätzen in Nr. 12 verrechnet werden kann. So ist bei $D = 131867$ für ungerade Formen und bei $fx = 3, fy = 11, fz = 17$, $3x - 3y \equiv o$, $3x + 3z \equiv o$, und es gibt sowohl $fx - y = (33, -23, 1003)$ als auch $fx + z = (51, -23, 649)$ eine Periode von 3 Gliedern.

c) Sind die Unbekannten so beschaffen, dass sich durch dieselben die Zeiger aller zu D gehörigen Primzahlen p, bei denen also nach Gauss $\left(\frac{-D}{p}\right) = 1$ ist, bis $\sqrt{\frac{D}{3}}$ bei ungeraden und $2\sqrt{\frac{D}{3}}$ bei geraden Formen, und falls man nicht so weit gehen könnte, doch wenigstens aller in der Rechnung vorkommenden angeben lassen, so kann man um θ zu finden, Folgendes als Grundsatz annehmen: „θ kann keine Zahl a zum Factor haben, wenn durch diese Annahme x, y, z etc. einen gemeinsamen Theiler erhalten würde;“ dann hätten nämlich diesen Theiler die Zeiger aller Primzahlen zum Factor, er würde daher auch bei allen Potenzen und Producten vorkommen, und θ wäre zu gross genommen. So kommen bei $D = 2653\ 71653$ für $fx = 3$ $fy = 11$, $fz = 13$ die Gleichungen $119x + 11y + 8z \equiv o$ $638x + 47y + 13z \equiv \frac{1}{3}\theta$, $385x + 31y + 4z \equiv o$ vor; die Elimination gibt $29724\,x \equiv o$, $29724\,y \equiv o$, $54494\,z \equiv o$. Das kleinste gemeinschaftliche Mittel dieser Coëfficienten ist

$$326964 = 2^2 \times 3 \times 11 \times 2477 = \lambda\theta.$$

Aber 4 ist kein Theiler von θ; denn zum Modell genommen würde es nach den obigen Gleichungen $x + y \equiv o$, $x - y \equiv o$ also $2x \equiv o$ liefern, wesshalb x, y und z gerade sein müsste.

Auch kann wegen der Congruenzen $3y + 2z \equiv o$ $-2y + 4z \equiv o$ (Mod. 11) oder $8y \equiv o$, die Zahl 11 kein Theiler von θ sein, und man findet $\theta = 14862$. Doch kommen ähnliche Untersuchungen bei kleinen Determinanten sehr selten vor.

Anmerkung. Hieraus ist ersichtlich, dass die Periodengleichungen die Eigenschaften der Periode und des Periodensystems enthalten, die man dann aus ihnen entwickeln kann.

15. Die reciproken Zahlen in den Perioden.

Zwei Zahlen D, N heissen bekanntlich reciprok, wenn N in den Formen der Determinante D und umgekehrt vorkommt. Eine quadra-

tische Zahlform enthält, wie bereits erwiesen ist, entweder keine oder lauter reciproke Zahlen. Hieran reihen sich folgende für die Reciprocität immerhin wichtigen Sätze:

a) Ist fn eine reciproke oder nicht reciproke Form, so ist es auch beziehungsweise $fn + 2m$, mag m welchen Werth immer haben. Hätte man nämlich $fn = N$ und $fm = M$, so gibt $fn + 2m = NM^2$, und man wird, wenn d was immer für eine in D aufgehende Primzahl ist, nach der Gauss'schen Bezeichnungsweise $\left(\frac{fn + 2m}{d}\right) = \left(\frac{NM^2}{d}\right) = \left(\frac{N}{d}\right) = \left(\frac{fn}{d}\right)$, daher auch $\left(\frac{-fn + 2m}{d}\right) = \left(\frac{-fn}{d}\right) = \pm 1$ haben. Es kommt also jede D theilende Primzahl, daher jede Potenz und jedes Product aus solchen Grössen in den Formen der Determinanten $fn + 2m$ vor oder nicht vor, je nachdem sich dieses bei fn ereignet.

b) Hat demnach D blos Perioden von einer ungeraden Länge, so wird entweder jede Form reciprok sein oder keine. Ersteres geschieht bei den Formen von der Gestalt $(2a, 2b, 2c)$, wenn D eine Primzahl oder Primpotenz von der linearen Form $8\varphi + 3$ ist, Letzteres bei den unpaaren und paaren Formen von $D = 8\varphi + 3$ und bei allen Formen der Determinanten $D = 8\varphi - 1$, mag D eine Primzahl sein oder nicht.

c) Ist $P = at^2 + btu + cu^2$ oder $4aP = (2at + bu)^2 + Du^2$ so hat man für jede Primzahl d, die D theilt $\left(\frac{4aP}{d}\right) = \left(\frac{aP}{d}\right) = 1$ also $\left(\frac{a}{d}\right) = \left(\frac{P}{d}\right)$. Da man nun bei jeder Form mit einem geraden Zeiger $P = p^2$ setzen kann, so ist $\left(\frac{a}{d}\right) = 1$ das Kennzeichen von $f2m = a$. Bei Formen mit einem ungeraden Zeiger muss nämlich immer $\left(\frac{a}{d}\right) = -1$ sein; denn wäre $\left(\frac{a}{d}\right) = 1$ also auch $\left(\frac{c}{d}\right) = 1$,

so übergeht $$p^2 = at^2 + btu + cu^2$$

wenn $$p = cz,\ t = 2cy,\ u = x - by$$

gesetzt wird, in $x^2 + Dy^2 = cz^2$, welche Gleichung nach Legendre Nr. 27 immer in Ansehung dessen, dass hier c eine Zahl der Determinante D ist, d. h. dass man für jede Primzahl c',

diese theilt, $\left(\frac{-D}{c'}\right) = 1$ erhält, in ganzen Zahlen lösbar ist. Man findet daher Werthe für p, t, u, und die gegebene Form ist wirklich $= p^2$, und hat also einen geraden Zeiger.

d) Ist die Periodenlänge eine gerade Zahl, so sind entweder alle Formen einer Periode mit geraden oder alle mit ungeraden Zeigern reciprok, oder es findet dies bei keiner derselben Statt; nie aber kann in einer solchen Periode eine Form mit einem paaren und eine mit unpaarem Zeiger zugleich reciprok sein. Ist nämlich $\left(\frac{-fn}{d}\right) = \left(\frac{-fm}{d}\right) = 1$, so wird man, wenn $fn = Hfm$ gesetzt wird, $\left(\frac{-Hfm}{d}\right) = \left(\frac{H}{d}\right)\left(\frac{-fm}{d}\right) = 1$ also $\left(\frac{H}{d}\right) = 1$ erhalten, wesshalb nach *c)* $H = f2\alpha$ zu nehmen ist, woraus dann $fn = f2\alpha + m$ oder $n = 2\alpha + m$ folgt, so dass n mit m immer nur gerade oder ungerade sein kann.

e) Ist $D = g^2 + h^2$, so hat, wie bekannt, jeder ungerade Theiler d dieser Determinante die Gestalt $4\varphi + 1$, und man erhält $\left(\frac{-[x^2 + Dy^2]}{d}\right) = \left(\frac{-x^2}{d}\right) = 1$. Desshalb ist dann die Schlussform und mit ihr jede Form, die einen geraden Zeiger besitzt, reciprok, indem die Schlussform in allen Perioden vorkommt. Hätte jedes d die Gestalt $8\varphi + 1$, so ist wegen $\left(\frac{-2}{d}\right) = 1$ die Mittelform $(2, 2, 4\varphi + 1)$ auch mit reciprok.

Wäre D nicht $= g^2 + h^2$ und auch nicht von der Gestalt $4\varphi - 1$ oder 4φ, so ist θ gerade und die reciproken Formen haben ungerade Zeiger.

Anmerkung. Da nach Legendre Nr. 302 etc. jede reciproke Form auch eine trinäre ist, so gilt alles von den ersteren Gesagte auch von den letzteren.

16. Formenzahl und Länge der Perioden.

a) In dieser Hinsicht verdient folgender von Dirichlet[1]) aufgefundene und von Lipschitz elementär erwiesene Satz eine

[1]) Crelle's Journal Band 21, S. 12 und Band 53, S. 255.

besondere Beachtung: „Ist h die Anzahl der Formen erster Art (d. h. der eigentlichen quadratischen) von der Determinante D, und h' die Anzahl der Formen erster Art von der Determinante $D' = DS^2$ wo S irgend eine ganze Zahl bedeutet, so ergibt sich die Beziehung, dass h' und h in einem angebbaren Verhältnisse stehen, und zwar, dass $h' = hl$ ist", wo bei negativen Determinanten

$$l = \left[r - \left(\frac{-D}{r}\right)\right]\left[r' - \left(\frac{-D}{r'}\right)\right]\left[r'' - \left(\frac{-D}{r''}\right)\right] \text{ etc.}$$

vorstellt, wenn man $S = rr'r''$ etc. hat. Hiebei ist nach Gauss $\left(\frac{-D}{r}\right) \equiv (-D)^{\frac{r-1}{2}} \equiv \pm 1 \pmod{r}$, welche Grösse Null zu setzen ist, wenn $r = 2$ oder ein Theiler von D ist. Was $D = S^2$ anbelangt, wenn S eine Primzahl ist, hat man $l = S - \left(\frac{-1}{S}\right)$ und $h' = \frac{l}{2}$, d. h. h' ist die gerade Zahl $\frac{S \pm 1}{2}$.

Dieses Gesetz hat jedoch seine Giltigkeit nur unter der Voraussetzung, dass die Formen (a, b, c) und $(a, -b, c)$ mit Ausnahme des besonderen Falles in Nr. 2 b ungleich sind. Daraus erhellet die Nothwendigkeit der Annahme von $fu - gm = 1$ in Nr. 1.

b) Mittelst des vorstehenden Satzes ist man in den Stand gesetzt, die Formenzahl bei Potenzen aus Primzahlen, und da letztere meistens nur eine Periode haben, die Länge derselben zu bestimmen: hat nämlich p, p^2 beziehungsweise θ, ϑ Formen, so wird die Anzahl der geraden Formen bei $D = p^{2n+1}$, $\theta' = \theta p^n$ und bei $D = p^{2n}$, $\theta' = \vartheta p^{n-1}$ betragen, wesshalb auch die Determinanten 2^{2n+1} und 2^{2n+2} eine Periode von 2^n Gliedern haben.

Was die ungeraden Formen anbelangt, beträgt ihre Anzahl bei den unpaaren Potenzen der Primzahl $p = 8\varphi + 3$ blos $\frac{1}{3}\theta p^n$ nämlich den dritten Theil der geraden, indem die drei geraden Formen $(4a, 2b, c)$, $(a, 2b, 4c)$, $(4a, -2[2a-b], a-b+c)$ in die ungerade (a, b, c) übergehen. Dies gilt offenbar auch bei $u = o$, da bei $D = p = 8\varphi + 3$ die Anzahl der ungeraden Formen $\frac{1}{3}\theta$ ist, wenn jene der geraden θ beträgt.

c) Hat die Determinante D mehr als eine Periode, so ist die Zahl der Formen durch die Gliederzahl der längsten daher auch jeder andern Periode theilbar.

Was das Periodensystem unter a Nr. 12 anbelangt, enthält es im Ganzen e^k Formen in Perioden von e Gliedern; erscheint dieses System mit einer θ gliedrigen Periode verbunden, so gibt es $e^k\,\theta$ Formen in $e\,\theta$ gliedrigen Perioden.

In der zweiten Gattung der Periodensysteme haben die e^a gliedrigen Perioden $(e-1)\,e^{a-1} \times e^k$ Formen, deren Zeiger durch e nicht theilbar sind, nebstdem haben sie eine e^{a-1} gliedrige Periode, deren Zeiger durch e aufgehen, gemeinschaftlich, daher im Ganzen

$$(e-1)\,e^{a-1} \times e^k + e^{a-1} = (e-1)\,(e^k-1)\,e^{a-1} + e^a$$

Formen. Die $e^{a-1}, e^{a-2}, \ldots . e^2$ gliedrigen Perioden enthalten beziehungsweise

$$(e-1)\,(e^k-1)\,e^{a-2},\ (e-1)\,(e^k-1)\,e^{a-3},\ \ldots .\ (e-1)\,(e^k-1)\,e$$

neue Formen, dazu gibt es noch

$$e\,(e^k-1) = (e-1)\,(e^k-1) + e^k - 1$$

Formen in e gliedrigen Perioden; daher beträgt die Anzahl sämmtlicher unter einander verschiedener Formen

$$(e^k-1)\,(e-1)\,[e^{a-1} + e^{a-2} + e^{a-3} + \ldots e + 1] + e^a + e^k - 1,$$

oder weil $e^{a-1} + e^{a-2} + e^{a-3} + \ldots e + 1 = \frac{e^a - 1}{e-1}$ ist, $(e^k-1)\,(e^a-1) + e^a + e^k - 1 = e^{a+k}$, welche Grösse sich offenbar durch e^a theilen lässt.

Eben so hat der obige Satz auch in dem Falle seine Richtigkeit, wenn das letztere Periodensystem mit einer θ gliedrigen Periode verbunden erscheint.

d) Ausser diesen berühren die Periodenlänge noch folgende specielle Sätze:

Ist $D = a^m - b^2$ und a ungerade, so ist θ durch m theilbar, weil hier die Periode
$(a, 2\,b, a^{m-1}), (a^2, 2\,b, a^{m-2}) \ldots . (a^m, 2\,b, 1)$ zum Vorschein kommt. Wäre jedoch $D = 2^m - b^2$, so wird $\theta = \lambda\,(m-2)$ sein, da die Formen $(2, b, 2^{m-3}), (4, b, 2^{m-4}) \ldots . (2^{m-2}, b, 1)$ eine

$(m-2)$ gliedrige Periode bilden. Aus ähnlichen Gründen haben $D = 4a^m - b^2$ und $D = 2a^m - b^2$ die Grössen μm und $2\mu m$ zu Periodenlängen.

Die Primzahl $D = 8\varphi + 1$ hat eine Periode von 4λ Gliedern, da nach Nr. 15 die Mittelform $(2, 2, 4\varphi + 1)$ reciprok ist, und desshalb einen geraden Zeiger hat. Wäre $D = 8\varphi + 5$ und Primzahl, so ist $\theta = 4\lambda + 2$, weil in diesem Falle die Mittelform nicht reciprok ist, daher einen ungeraden Zeiger besitzt, wie dies in diesen beiden Fällen aus der Reciprocität von $(1, D)$ hervorgeht.

Beide letzteren Fälle gelten auch von allen Potenzen und Producten, wenn die Wurzeln und einfachen Factoren dieselben Eigenschaften wie D besitzen, so wie auch bei dem Doppelten derartiger Grössen.

17. Bemerkungen über die Determinanten in Hinsicht ihrer Theilbarkeit.

Will man eine ungerade Zahl in zwei Factoren zerlegen, so reicht es hin zu ihr als Determinante eine Mittelform ausser $\left(2, 2, \frac{D+1}{2}\right)$ aufzusuchen, indem nach Nr. 2 die Mittelformen (p, p, r), (p, q, p), (p, r), $(2p, 2p, r)$, $(p, 2q, p)$ beziehungsweise $D = p(4r - p)$, $(2p - q)(2p + q)$, pr, $p(2r - p)$, $(p - q)(p + q)$ geben.

Kommt bei D keine dieser Mittelformen vor, so kann es nur eine Primzahl oder Primpotenz sein. Gerade Potenzen sind vollständige Quadrate, und die ungeraden erkennt man daran, dass sie mit ihrer Periodenlänge die Wurzel oder eine ihrer Potenzen gemein haben.

Da mittelst der Bestimmbarkeit der Formen und der Periodengleichungen die Verrechnung der Perioden bedeutend erleichtert wird, so ist man auch in den Stand gesetzt, sehr grosse Zahlen in Factoren zu zerlegen oder ihre Primität zu erkennen. Auf diese Weise wurde unter andern auch

$11111111111111111 = \frac{1}{9}(10^{17} - 1) = 2071723 \times 5363222357$

zerlegt, welches wohl die grösste Zahl ist, bei der dies ohne Zufall geschah.

Anmerkung. Bei Zahlenzerlegungen nach dieser Methode finde man oft $f2a = m^2$, oder es lässt sich aus den Bestim-

mungsgleichungen eine solche Form ableiten; dann hat man $\frac{f^2 a}{m^2} = \left(\frac{fa}{m}\right)^2 = 1$, und es kann $fa : m$ blos eine Schluss- oder Mittelform sein. Gewöhnlich ist das letztere der Fall. Seltener trifft es sich, dass man zu einer Form von der Gestalt (aa^2, b, ac^2), wo daher $D = (2aac - b)(2aac + b)$ ist, gelangt, oder dass in (a, b, c) a mit b oder b mit c einen gemeinsamen Theiler hat, der demnach auch D theilt.

18. Unbestimmte Gleichungen von der Gestalt $pz^m = ax^2 + bxy + cy^2$.

Zur Lösbarkeit dieser Gleichung ist vorerst erforderlich, dass p mit (a, b, c) zu derselben Determinante gehöre; denn aus $4acpz^m = (2ax + by)^2 + Dy^2 = M^2 + Dy^2$ folgt, wenn p' was immer für eine p theilende Primzahl ist

$$\left(\frac{-Dy^2}{p'}\right) = \left(\frac{-D}{p'}\right) = \left(\frac{M^2}{p'}\right) = 1.$$

Eben so sieht man, dass jeder Werth von z dieser Determinante zugehören werde. Ist nun in der Periode oder im Periodensystem, welches bei $D = 4ac - b^2$ oder falls $b = 2b'$ wäre, bei $D = ac - b'^2$ vorkommt,

$$fa = (a, b, c) \text{ und } p = a'f^2 + b'fg + c'g^2 = f\beta,$$

wo also β je nach der Beschaffenheit von p auch mehrere Werthe haben kann, so wird man $z^m = f(\alpha \mp \beta)$ erhalten, indem pz^m keine Bestimmungsgrösse (Nr. 9) sondern ein blosses Product ist. Setzt man weiter $z = fw$ oder $z^m = f^m w$, so ergibt sich $mw \equiv \alpha \mp \beta$ (Mod. θ). Zur Lösbarkeit dieser Congruenz ist demnach erforderlich, dass der grösste gemeinschaftliche Theiler von m, θ in $\alpha \mp \beta$ aufgehe. Hat man auf diese Weise einen oder mehrere Werthe von w gefunden, so liefert die Periode oder das Periodensystem für jedes w eine Form von der Gestalt $z = fw = kt^2 + ntu + ru^2$, wo k, n, r bestimmte, t, u hingegen willkürliche Grössen sind. Erhebt man diese Gleichung zur m^{ten} Potenz, und multiplicirt dann das Resultat mit $f^{\pm}\beta = (a', \pm b', c')$, so kommt nach den gehörigen Reductionen $f(mw \pm \beta) = fa = ax^2 + bxy + cy^2$ zum

Vorschein, wobei die Unbekannten x, y, durch Functionen des m^{ten} Grades von t, u dargestellt sind.

Beispiel: $37z^3 = 3x^2 + 2xy + 34y^2$.

Hier gibt $D = 101$ für $f1 = (3, 2, 34)$ eine Periode von 14 Gliedern, worin $f8 = (6, 2, 17) = 37$ bei $x' = 2$, $y' = -1$ vorkommt. Daraus folgt $3w \equiv 1 \mp 8 \pmod{14}$ oder $3w \equiv 21$ vel 9 und $w = 7, 3$. Daher ist vorerst $z = f7 = 2t^2 + 2tu + 51u^2$, daraus findet man $z^3 = 2X^2 + 2XY + 51Y^2$,

wo $X = 2t^3 - 153tu^2 - 51u^3$ und $Y = 6t^2u + 6tu^2 - 49u^3$;

folglich $37z^3 = (2X^2 + 2XY + 51Y^2)(17y'^2 - 2x'y' + 6x'^2)$,

was $$37z^3 = 3x^2 + 2xy + 34y^2$$

gibt, wobei

$$x = 8t^3 + 102t^2u - 510tu^2 - 1037u^3.$$
$$y = -2t^3 + 30t^2u + 183tu^2 - 194u^3.$$

Eben so findet man die zweite Lösungsweise für

$$z = f_3 = 10t^2 - 6tu + 11u^2$$
$$x = -96t^3 + 258t^2u + 162tu^2 - 127u^3$$
$$y = -14t^3 - 78t^2u + 93tu^2 + 10u^3.$$

Anmerkung. Mehreres über Gleichungen dieser Art, besonders was den Fall von $m = 2$ anbelangt zu erwähnen, ist wohl nicht nöthig, da hierüber Gauss, Lagrange, Legendre und neulich Herrmann Scheffler in seiner „unbestimmten Analytik (Hannover 1854) weitläufig genug gehandelt haben. Was jedoch die vorstehende Methode anbelangt, so gibt es, wenn $m > 2$ vorkommt, keine bessere; überdies ist sie sowohl bei sehr grossen als auch bei positiven Determinanten brauchbar, indem letztere auch Perioden- und Periodensysteme besitzen; und wenn sie auch in der bündigen Darstellung der Resultate einigen andern Methoden nachsteht, so gewährt sie dafür wieder die Sicherheit keine Lösungsweise übergangen zu haben.