Werk

Titel: Vorlesungen über Zahlentheorie
Autor: Dirichlet, Peter
Verlag: Vieweg
Ort: Braunschweig
Jahr: 1871
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN30976923X
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN30976923X
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=30976923X

LOG Id: LOG_0175
LOG Titel: §. 156. Ableitung aller Lösungen der Gleichung ax^2 + by^2 + cz^2 = 0 aus einer gegebenen
LOG Typ: chapter

Contact

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

durch Duplication der Form (x, x', xx'') entsteht; mithin ist $Q = K^2$, wo K die Classe bedeutet, welcher die Form (x, x', xx'') angehört. Das obige zu beweisende Theorem ist daher identisch mit dem folgenden:

Ist (A, B, C) eine Form des Hauptgeschlechtes der Determinante D, so ist die Gleichung

$$Az^2 + 2Bzy + Cy^2 = x^2$$

stets lösbar in ganzen Zahlen z, y, x, deren letzte relative Primzahl zu $2D$ ist.

§. 156.

Durch die vorstehende Betrachtung sind wir dahin geführt, die Lösbarkeit einer Gleichung von der Form

$$ax^2 + by^2 + cz^2 + 2a'yz + 2b'zx + 2c'xy = 0$$

in ganzen Zahlen x, y, z (oder was Dasselbe ist, die Lösbarkeit der allgemeinen Gleichung

$$au^2 + bv^2 + 2c'uv + 2b'u + 2a'v + c = 0$$

in *rationalen* Zahlen u, v) zu untersuchen. Dieselbe kann, allgemein zu reden, auf den speciellen Fall zurückgeführt werden, in welchem die Coefficienten a', b', $c' = 0$ sind*), und wir beschäftigen uns daher im Folgenden nur mit Gleichungen von der Form

$$ax^2 + by^2 + cz^2 = 0, \qquad (1)$$

wo a, b, c drei gegebene, von Null verschiedene ganze Zahlen bedeuten, die wir ausserdem stets als *relative Primzahlen* annehmen, weil jeder andere Fall, wie man leicht erkennt, sich auf diesen zurückführen lässt**). Wir wollen nun eine Lösung x, y, z eine *eigentliche* Lösung nennen, wenn die drei Zahlen x, y, z *relative Primzahlen* sind; dann leuchtet ein, dass ax, by, cz ebenfalls relative Primzahlen sind; ginge nämlich eine Primzahl p in zweien von ihnen auf, so müsste p zufolge (1) auch in der dritten aufgehen; da aber höchstens einer der Coefficienten a, b, c durch p

*) *Gauss: D. A.* artt. 299, 300.

**) *Gauss: D. A.* art. 298.

theilbar sein kann, so wären wenigstens zwei der Zahlen x, y, z theilbar durch p, also keine relative Primzahlen.

Nach dieser Vorbemerkung beginnen wir unsere Untersuchung*), indem wir uns die folgende Aufgabe stellen:

I. *Aus einer gegebenen eigentlichen Lösung* $x = u$, $y = v$, $z = w$ *der Gleichung* (1) *ihre sämmtlichen Lösungen abzuleiten.*

Da au, bv, cw relative Primzahlen sind, und eine von ihnen, z. B. au, zufolge der Gleichung

$$au^2 + bv^2 + cw^2 = 0 \tag{2}$$

gerade ist, so haben auch die Zahlen $2au$, bv, cw keinen gemeinschaftlichen Theiler, und man kann daher (nach §. 24) die Gleichung

$$aul + bvm + cwn = 1$$

so lösen, dass l gerade, und folglich die eine der beiden Zahlen m, n gerade, die andere ungerade wird; setzt man nun

$$al^2 + bm^2 + cn^2 = h$$

und

$$u' = 2l - hu,\ v' = 2m - hv,\ w' = 2n - hw,$$

so wird h ungerade, und man erhält**)

$$au'^2 + bv'^2 + cw'^2 = 0 \tag{3}$$

$$auu' + bvv' + cww' = 2 \tag{4}$$

$$u \equiv u',\ v \equiv v',\ w \equiv w' \pmod 2; \tag{5}$$

man kann daher

$$vw' - wv' = 2u'',\ wu' - uw' = 2v'',\ uv' - vu' = 2w'' \tag{6}$$

setzen, wo u'', v'', w'' ganze Zahlen bedeuten, welche mit den andern noch durch folgende Relationen***) verbunden sind:

---

*) Sie ist der Kürze halber synthetisch geführt; derselbe Gegenstand ist auf andere Weise behandelt in der mir erst nachträglich bekannt gewordenen Abhandlung von *G. Cantor: De aequationibus secundi gradus indeterminatis.* 1867.

**) Umgekehrt lässt sich aus (2), (3), (4), (5) leicht beweisen, dass a, b, c relative Primzahlen sind, und dass sowohl u, v, w, als auch u', v', w' eigentliche Lösungen der Gleichung (1) bilden; doch ist dies für unsere Zwecke nicht nöthig.

***) Man findet z. B. die erste der Gleichungen (7) aus der identischen Gleichung

$$(bv^2 + cw^2)(bv'^2 + cw'^2) = (bvv' + cww')^2 + bc(vw' - wv')^2$$

unter Berücksichtigung von (2), (3), (4), (6); die Gleichung (8) ergiebt sich

$$\left.\begin{aligned} auu' &= 1 + bcu''^2 \\ bvv' &= 1 + cav''^2 \\ cww' &= 1 + abw''^2 \end{aligned}\right\} \tag{7}$$

$$bcu''^2 + cav''^2 + abw''^2 = -1 \tag{8}$$

$$\left.\begin{aligned} vw' + wv' &= 2av''w'' \\ wu' + uw' &= 2bw''u'' \\ uv' + vu' &= 2cu''v'' \end{aligned}\right\} \tag{9}$$

Mit Hülfe derselben ist es leicht, unsere Aufgabe allgemein zu lösen. Sind x, y, z drei beliebige ganze Zahlen, so werden auch

$$\left.\begin{aligned} t &= au'x + bv'y + cw'z \\ t' &= aux + bvy + cwz \\ t'' &= u''x + v''y + w''z \end{aligned}\right\} \tag{10}$$

ganze Zahlen, welche zufolge (5) der Bedingung

$$t \equiv t' \pmod 2 \tag{11}$$

genügen; umgekehrt, sind t, t', t'' drei beliebige ganze Zahlen, welche nur der Bedingung (11) unterworfen sind, so folgt aus (10) unter Berücksichtigung von (5), (7) und (9), dass

$$\left.\begin{aligned} 2x &= ut + u't' - 2bcu''t'' \\ 2y &= vt + v't' - 2cav''t'' \\ 2z &= wt + w't' - 2abw''t'' \end{aligned}\right\} \tag{12}$$

gerade, also x, y, z ganze Zahlen sind. Multiplicirt man diese letzten Gleichungen resp. mit ax, by, cz, und addirt mit Rücksicht auf (10), so folgt

$$ax^2 + by^2 + cz^2 = tt' - abct''^2;$$

mithin haben wir folgendes Resultat: *Bilden die ganzen Zahlen x, y, z eine Lösung der Gleichung* (1), *so werden t, t', t'' vermöge* (10) *ganze Zahlen, welche den Bedingungen* (11) *und*

$$tt' = abct''^2 \tag{13}$$

genügen; umgekehrt, befriedigen die ganzen Zahlen t, t', t'' die Be-

---

durch Addition aus (7) mit Rücksicht auf (4); und die erste der Gleichungen (9) folgt aus der Identität

$$(auu' + bvv' + cww')(vw' + wv') - a(wu' - uw')(uv' - vu') = (au^2 + bv^2 + cw^2)v'w' + (au'^2 + bv'^2 + cw'^2)vw.$$

dingungen (11) *und* (13), *so werden* x, y, z *vermöge* (12) *ganze Zahlen, welche der Gleichung* (1) *genügen**).

Zur Vervollständigung fügen wir hinzu: *Damit die Zahlen* x, y, z *eine eigentliche Lösung der Gleichung* (1) *bilden, ist ferner erforderlich und hinreichend, dass die Zahlen* t, t' *keinen ungeraden gemeinschaftlichen Theiler haben, und dass, wenn beide gerade sind,*

$$t + t' \equiv 2 \pmod{4} \qquad (14)$$

ist.

Für unsern Zweck genügt es zu beweisen, dass die beiden angegebenen Bedingungen hinreichend sind. Gesetzt, es ginge eine Primzahl p in zweien der Zahlen ax, by, cz auf, so müsste sie zufolge (1) auch in der dritten aufgehen, mithin zufolge (10) auch in t und t'; da aber t, t' der Annahme nach keinen ungeraden gemeinschaftlichen Theiler haben, so müsste $p = 2$ sein, und es wären also t, t', ax, by, cz gerade Zahlen; dann würde aber aus (10) mit Rücksicht auf (5) folgen, dass $t + t' \equiv 0 \pmod 4$ wäre, während wir doch angenommen haben, dass $t + t' \equiv 2 \pmod 4$ ist, sobald t und t' gerade Zahlen sind. Hieraus folgt also, dass ax, by, cz relative Primzahlen sind, was zu beweisen war**).

---

*) Die allgemeinste Lösung der Gleichung (13), deren wir zwar in der Folge nicht bedürfen, besteht, wie man sehr leicht findet, in den Gleichungen

$$t = \tau d \omega^2, \quad t' = \tau d' \omega'^2, \quad t'' = \tau \omega \omega',$$

wo $d, d', \tau, \omega, \omega'$ beliebige ganze Zahlen bedeuten, welche der einzigen Bedingung

$$d d' = abc$$

unterworfen sind; man kann aber auch, ohne die Allgemeinheit zu beeinträchtigen, annehmen, dass τ der grösste gemeinschaftliche Theiler von t, t', t'', und dass τd, $\tau d'$ die grössten Theiler sind, welche τabc resp. mit t, t' gemeinschaftlich hat. Führt man diese Ausdrücke in (12) ein, so erhält man die binären quadratischen Formen

$$\frac{2x}{\tau} = (du, -bcw'', d'u'), \quad \frac{2y}{\tau} = (dv, -cav'', d'v'),$$
$$\frac{2z}{\tau} = (dw, -abw'', d'w'),$$

deren Variabeln ω, ω', und deren Determinanten zufolge (7) die Zahlen $-bc$, $-ca$, $-ab$ sind. Transformirt man diejenige dieser Formen, deren Determinante negativ ist, in eine reducirte Form (§. 64), so erhält man die einfachsten Lösungen.

**) Es ist leicht, wenn auch für unsern Zweck nicht erforderlich, die beiden angegebenen Bedingungen auf die Zahlen $d, d', \tau, \omega, \omega'$ zu übertragen: die Zahlen d, d' müssen relative Primzahlen sein, und nur, wenn

II. Bilden die Zahlen x, y, z eine eigentliche Lösung der Gleichung (1), so sind ax, by, cz relative Primzahlen, und man kann folglich drei Zahlen $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ bestimmen, welche den Congruenzen

$$\mathfrak{A}z \equiv by \pmod{a}, \quad \mathfrak{B}x \equiv cz \pmod{b}, \quad \mathfrak{C}y \equiv ax \pmod{c} \tag{15}$$

genügen, woraus in Verbindung mit (1)

$$\mathfrak{A}^2 \equiv -bc \pmod{a}, \quad \mathfrak{B}^2 \equiv -ca \pmod{b}, \quad \mathfrak{C}^2 \equiv -ab \pmod{c} \tag{16}$$

folgt. Wir haben mithin folgenden Satz erhalten:

Ist die Gleichung (1) *eigentlich lösbar, so sind die Zahlen* $-bc, -ca, -ab$ *resp. quadratische Reste der Zahlen* a, b, c, *und jede eigentliche Lösung* x, y, z *führt durch die Congruenzen* (15) *zu drei völlig bestimmten Zahlclassen* $\mathfrak{A}$ *(mod.* a*),* $\mathfrak{B}$ *(mod.* b*),* $\mathfrak{C}$ *(mod.* c*), welche den Congruenzen* (16) *genügen**).

Von der grössten Wichtigkeit für unsere Untersuchungen ist es aber, dass dieser Satz sich in folgender Weise umkehren lässt:

Ist die Gleichung (1) *eigentlich lösbar, und sind drei Zahlen* $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ *gegeben, welche den Congruenzen* (16) *genügen, so kann man stets eigentliche Lösungen* x, y, z *finden, welche die Bedingungen* (15) *erfüllen.*

Um dies zu beweisen, bestimmen wir zunächst drei Zahlen X, Y, Z durch die (nach §. 25) stets vereinbaren Congruenzpaare

$$\left.\begin{array}{lll} X \equiv c \pmod{b}, & Y \equiv a \pmod{c}, & Z \equiv b \pmod{a} \\ X \equiv \mathfrak{C} \pmod{c}, & Y \equiv \mathfrak{A} \pmod{a}, & Z \equiv \mathfrak{B} \pmod{b} \end{array}\right\} \tag{17}$$

aus welchen unter Berücksichtigung der Annahme (16) die der Gleichung (1) ähnliche Congruenz

$$aX^2 + bY^2 + cZ^2 \equiv 0 \pmod{abc} \tag{1'}$$

folgt, weil ihre linke Seite durch jede der drei relativen Primzahlen a, b, c theilbar ist. Da ferner die Existenz einer eigentlichen Lö-

---

$abc \equiv 0 \pmod{8}$, können sie auch den grössten gemeinschaftlichen Theiler 2 haben; umgekehrt, genügt die Zerlegung $abc = dd'$ diesen Bedingungen, so kann man τ, ω, ω' so wählen, dass x, y, z eine eigentliche Lösung der Gleichung (1) bilden.

*) Wirft man zwei eigentliche Lösungen in dieselbe oder in verschiedene *Classen*, je nachdem sie zu denselben drei Zahlclassen $\mathfrak{A}$ (mod. a), $\mathfrak{B}$ (mod. b), $\mathfrak{C}$ (mod. c) führen oder nicht, so ist die Anzahl aller verschiedenen Classen *höchstens* gleich der Anzahl der incongruenten Wurzeln der Congruenz $x^2 \equiv 1 \pmod{abc}$, und der nachfolgende Satz behauptet die wirkliche Existenz aller dieser Classen von eigentlichen Lösungen.

sung u, v, w der Gleichung (1) angenommen ist, so behalten wir alle früheren Bezeichnungen bei und setzen

$$\left.\begin{aligned} T &\equiv au'X + bv'Y + cw'Z \\ T' &\equiv auX + bvY + cwZ \end{aligned}\right\} \text{(mod. } 2abc\text{)}, \qquad (10')$$

woraus zufolge (5)

$$T \equiv T' \text{ (mod. 2)} \qquad (11')$$

und mit Rücksicht auf (7) und (9)

$$\left.\begin{aligned} 2X &\equiv uT + u'T' \text{ (mod. } 2bc\text{)} \\ 2Y &\equiv vT + v'T' \text{ (mod. } 2ca\text{)} \\ 2Z &\equiv wT + w'T' \text{ (mod. } 2ab\text{)} \end{aligned}\right\} \qquad (12')$$

folgt; multiplicirt man diese Congruenzen resp. mit aX, bY, cZ, wodurch sie in Congruenzen nach dem Modulus $2abc$ übergehen, so ergiebt sich durch Addition unter Berücksichtigung von (1') und (10')

$$TT' \equiv 0 \text{ (mod. } abc\text{)}. \qquad (13')$$

Wir behaupten nun, dass die drei Zahlen T, T', abc keinen ungeraden gemeinschaftlichen Divisor haben, und dass, wenn abc gerade ist,

$$T + T' \equiv 2 \text{ (mod. 4)} \qquad (14')$$

ist. Ginge nämlich eine ungerade Primzahl p in T, T' und abc, also auch z. B. in c auf, so würde Y zufolge (12') durch p theilbar sein, und da $a \equiv Y$ (mod. c) ist, so hätten a und c den gemeinschaftlichen Theiler p, was unmöglich ist. Wenn ferner abc, und also auch z. B. c gerade ist, so sind zufolge (11') und (13') auch T und T' gerade Zahlen; wäre nun die Congruenz (14') unrichtig, so wäre $T' \equiv T$ (mod. 4), und aus (12') würde folgen, dass $2Y \equiv (v + v')T \equiv 0$ (mod. 4), also Y gerade wäre, was abermals gegen die Congruenz $a \equiv Y$ (mod. c) streitet, weil a relative Primzahl zu c ist.

Nach diesen Vorbereitungen sind wir im Stande, eine eigentliche Lösung x, y, z nachzuweisen, welche den Bedingungen (15) genügt; diese letztern gehen vermöge der Definition (17) der Zahlen X, Y, Z in die folgenden über

$$Yz \equiv Zy \text{ (mod. } a\text{)}, \quad Zx \equiv Xz \text{ (mod. } b\text{)}, \quad Xy \equiv Yx \text{ (mod. } c\text{)};$$

da ferner aus den Definitionen (10) und (10') der Zahlen t, t' T, T' die Congruenz

$$\left.\begin{array}{l} T't - Tt' \equiv \\ 2bcu''(Yz - Zy) + 2cav''(Zx - Xz) + 2abw''(Xy - Yx) \end{array}\right\} (\mathrm{mod.}\, 2abc)$$

folgt, und da u'', v'', w'' zufolge (7) resp. relative Primzahlen zu a, b, c sind, so fallen die von x, y, z zu erfüllenden Bedingungen (15) durchaus mit der einzigen Forderung

$$T't \equiv Tt' \ (\mathrm{mod.}\ 2abc)$$

zusammen, welcher die Zahlen t, t' genügen müssen; sollen ferner die Zahlen x, y, z eine eigentliche Lösung der Gleichung (1) bilden, so haben t und t' ausserdem noch die früher erwähnten Bedingungen (11), (13), (14) zu erfüllen. Dies Alles lässt sich in der That auf folgende Weise erreichen.

Ist abc ungerade, so sei d der grösste gemeinschaftliche Theiler der beiden Zahlen T und $abc = dd'$; da nun zufolge (13') TT' durch abc theilbar ist, so geht d' in T' auf, und da, wie oben gezeigt ist, die Zahlen T, T', abc keinen ungeraden gemeinschaftlichen Theiler haben, so sind d und d' relative Primzahlen, und d' ist zugleich der grösste gemeinschaftliche Theiler der beiden Zahlen T' und abc. Dann leuchtet ein, dass man allen Forderungen genügt, wenn man z. B. $t = d$, $t' = d'$, $t'' = 1$ nimmt; denn weil $t \equiv t' \equiv 1$ (mod. 2), so werden x, y, z ganze Zahlen, die wegen $tt' = abct''^2$ eine Lösung der Gleichung (1) bilden; diese Lösung ist eine eigentliche, weil t, t' ungerade relative Primzahlen sind; da endlich $t \equiv t'$, $T \equiv T'$ (mod. 2), und $T't \equiv Tt' \equiv 0$ (mod. dd') ist, so folgt auch $T't \equiv Tt'$ (mod. $2abc$) d. h. die eigentliche Lösung x, y, z genügt den vorgeschriebenen Congruenzen (15).

Ist aber abc, und folglich auch T, T' gerade, und zwar $T + T' \equiv 2$ (mod. 4), so können wir der Symmetrie wegen annehmen, es sei $T \equiv 0$, $T' \equiv 2$ (mod. 4); dann sei d wieder der grösste gemeinschaftliche Theiler der beiden Zahlen T und $abc = dd'$, so wird d' in T' aufgehen. Ist nun d' ungerade, so genügt man allen Bedingungen, wenn man z. B. $t = 2d$, $t' = 2d'$, $t'' = 2$ nimmt; denn es ist $t \equiv 0$, $t' \equiv 2$ (mod. 4), $tt' = abct''^2$, $T't \equiv Tt' \equiv 0$ (mod. $2abc$), und t, t' haben keinen ungeraden gemeinschaftlichen Theiler. Ist aber d' gerade, so kann man wieder durch $t = d$, $t' = d'$, $t'' = 1$ allen Bedingungen genügen; da nämlich $T : d$ relative Primzahl zu d' und folglich ungerade ist, so muss, weil $T \equiv 0$ (mod. 4), auch $d \equiv 0$ (mod. 4) sein; da ferner d' in T' aufgeht, und $T' \equiv 2$ (mod. 4) ist, so muss auch $d' \equiv 2$ (mod. 4) sein; mithin ist $t \equiv 0$, $t' \equiv 2$ (mod. 4); es ist ferner $tt' = abct''^2$, und

die Zahlen t, t' haben keinen ungeraden gemeinschaftlichen Theiler; da endlich die Quotienten $T:d$ und $T':d'$ ungerade sind, so ist ihre Differenz gerade, und folglich, wenn man mit $dd' = abc$ multiplicirt, $Td' - T'd = Tt' - T't \equiv 0 \pmod{2abc}$, was zu beweisen war.

Es hat keine Schwierigkeit, ausser den eben angegebenen speciellen Lösungen, welche die vorgeschriebenen Congruenzen (15) erfüllen, alle andern zu bestimmen, und man findet namentlich leicht, dass zwei eigentliche Lösungen x, y, z und x_1, y_1, z_1, welche resp. durch die Werthe t, t', t'' und t_1, t_1', t_1'' hervorgebracht werden, stets und nur dann denselben Congruenzen (15) genügen, wenn $tt_1' \equiv t't_1 \pmod{2abc}$ ist*); allein alle diese an sich interessanten Vervollständigungen sind für unsere Zwecke nicht erforderlich. Wir begnügen uns daher, aus den obigen Resultaten noch den Beweis des folgenden Satzes abzuleiten, dessen wir später durchaus bedürfen.

III. *Ist die Gleichung* (1) *eigentlich lösbar, und ist* $-bc$ *quadratischer Rest von* ap^2, *wo* p *eine in* bc *nicht aufgehende Primzahl bedeutet, so besitzt die Gleichung* (1) *auch solche eigentliche Lösungen* x, y, z, *welche der Bedingung* $x \equiv 0 \pmod{p}$ *genügen.*

Der Annahme zufolge besitzt die Gleichung (1) eine eigentliche Lösung u, v, w, und wir können alle hieraus in I. gezogenen Folgerungen für uns in Anspruch nehmen; es versteht sich von selbst, dass wir den vorstehenden Satz nur für den Fall zu beweisen brauchen, dass keine der beiden Zahlen u, u' durch p theilbar ist.

Ist nun p ungerade, so kann man, da der Annahme nach $-bc \equiv \alpha^2 \pmod{p}$ ist, das Vorzeichen von α so wählen, dass $bcu'' + \alpha$ nicht theilbar durch p ist; wären nämlich beide Zahlen

*) Hieraus folgt, dass allen zu derselben Classe gehörigen eigentlichen Lösungen dieselbe Zerlegung $abc = dd'$ entspricht, mit einziger Ausnahme des Falles, wo $abc \equiv 2 \pmod{4}$, in welchem der Factor 2 nach Belieben in d oder in d' aufgenommen werden kann, ohne dass eine Aenderung der Classe eintritt. Auf diese Weise ergiebt sich (vergl. die früheren Noten), dass die Anzahl der wesentlich verschiedenen Zerlegungen, und also auch die der wirklich existirenden Classen genau mit der Anzahl der incongruenten Wurzeln der Congruenz $x^2 \equiv 1 \pmod{abc}$ übereinstimmt; hierin liegt also ein neuer Beweis des obigen Satzes. Aber es schien angemessener, ihn so zu führen, dass zugleich eine Lösung gefunden wird, welche den vorgeschriebenen Congruenzen genügt.

$bcu'' + \alpha$ und $bcu'' - \alpha$ durch p theilbar, so müsste auch ihre Differenz 2α, also auch α durch die ungerade Primzahl p theilbar sein, was gegen $-bc \equiv \alpha^2 \pmod{p}$ und die Annahme streitet, dass p nicht in bc aufgeht. Da nun u ebenfalls nicht durch p theilbar ist, so kann man eine Zahl ω stets so bestimmen (§. 25), dass sie der Congruenz

$$u\omega \equiv bcu'' + \alpha \pmod{p}$$

genügt und ausserdem relative Primzahl zu $2abc$ wird, weil ω, falls p in $2abc$, also in a aufgehen sollte, schon vermöge dieser Congruenz relative Primzahl zu p wird. Setzt man nun

$$t = \tau\omega^2, \quad t' = \tau abc, \quad t'' = \tau\omega,$$

wo $\tau = 1$ oder $= 2$ zu nehmen ist, je nachdem abc ungerade oder gerade ist, so erhält man eine entsprechende eigentliche Lösung x, y, z, welche auch der Bedingung $x \equiv 0 \pmod{p}$ genügt. Ist nämlich abc ungerade, also $\tau = 1$, so ist $t \equiv t' \equiv 1 \pmod{2}$; ist aber abc gerade, also $\tau = 2$, so ist $t \equiv 2$, $t' \equiv 0 \pmod{4}$; da ferner ω relative Primzahl zu abc ist, so haben t, t' keinen ungeraden gemeinschaftlichen Divisor, und da $tt' = abct''^2$ ist, so bilden x, y, z eine eigentliche Lösung der Gleichung (1). Nun ist nach (12)

$$\begin{aligned} 2x &= ut + u't' - 2bcu''t'' \\ &= \tau(u\omega^2 - 2bcu''\omega + abcu') \end{aligned}$$

also mit Rücksicht auf (7)

$$2ux = \tau\{(u\omega - bcu'')^2 + bc\} \equiv 0 \pmod{p},$$

weil $u\omega - bcu'' \equiv \alpha$, $bc \equiv -\alpha^2$ ist; da endlich $2u$ nicht durch p theilbar ist, so folgt hieraus $x \equiv 0 \pmod{p}$.

Wir gehen jetzt zu dem Falle $p = 2$ über. Ist erstens a gerade, aber nicht $\equiv 0 \pmod{8}$, so ergiebt sich leicht, da der Annahme nach $-bc$ quadratischer Rest von $4a$, also $bc \equiv -1 \pmod{8}$ ist, dass u gar nicht ungerade sein kann; da nämlich a gerade, also bv, cw ungerade sind, und $b \equiv -c \pmod{8}$ ist, so folgt aus $au^2 + bv^2 + cw^2 = 0$, dass $au^2 \equiv 0 \pmod{8}$, und folglich, da a nicht $\equiv 0 \pmod{8}$ ist, jedenfalls u gerade sein muss; und offenbar haben dann alle anderen eigentlichen Auflösungen x, y, z dieselbe Eigenschaft $x \equiv 0 \pmod{2}$. Ist zweitens $a \equiv 0 \pmod{8}$, also $-bc \equiv 1 \pmod{8}$, so nehme man $t'' = 1$, und $tt' = abc$ der Art, dass einer der beiden Factoren, z. B. $t \equiv 2 \pmod{4}$, also der andere $t' \equiv 0 \pmod{4}$ wird, und dass sie keinen ungeraden gemeinschaftlichen Divisor erhalten, was sich stets erreichen lässt.

Hieraus folgt, dass die Zahlen x, y, z eine eigentliche Lösung bilden werden. Da nun der Voraussetzung nach u ungerade ist, und da aus $1 + bcu''^2 = auu' \equiv 0 \pmod 8$ folgt, dass auch u'' ungerade ist, so ergiebt sich

$$2x = ut + u't' - 2bcu''t'' \equiv 2 + 0 - 2 \equiv 0 \pmod 4,$$

also ist $x \equiv 0 \pmod 2$. Ist endlich drittens a ungerade, und $-bc$ quadratischer Rest von $4a$, also $bc \equiv -1 \pmod 4$, so nehme man $t'' = 1$, und nach Belieben $tt' = abc$, nur so, dass t und t' relative Primzahlen werden; dann bilden x, y, z eine eigentliche Lösung, weil ausserdem $t \equiv t' \equiv 1 \pmod 2$ ist. Da nun der Voraussetzung nach keine der Zahlen u, u' gerade ist, so folgt aus $auu' = 1 + bcu''^2$, dass u'' gerade, und folglich $auu' \equiv 1 \pmod 4$ ist; mithin ist $ut.u't' = auu'.bc \equiv -1 \pmod 4$, also $ut \equiv -u't' \pmod 4$, und hieraus ergiebt sich

$$2x = ut + u't' - 2bcu''t'' \equiv 0 \pmod 4,$$

also ist $x \equiv 0 \pmod 2$.

Hiermit ist der obige Satz vollständig bewiesen, und dieser Beweis enthält offenbar eine Methode, aus einer eigentlichen Lösung u, v, w einer Gleichung, deren Coefficienten a, b, c sind, eine eigentliche Lösung $x:p$, y, z derjenigen Gleichung abzuleiten, deren Coefficienten ap^2, b, c sind, vorausgesetzt, dass $-bc$ quadratischer Rest von ap^2 und nicht durch die Primzahl p theilbar ist. Durch wiederholte Anwendung desselben Satzes gelangt man offenbar zu folgendem Resultat:

Sind die Zahlen $A = aP^2$, $B = bQ^2$, $C = cR^2$ *relative Primzahlen, und sind die Zahlen* $-BC$, $-CA$, $-AB$ *resp. quadratische Reste von* A, B, C, *so folgt aus der Existenz einer eigentlichen Lösung der Gleichung*

$$ax^2 + by^2 + cz^2 = 0$$

stets die Existenz einer eigentlichen Lösung der Gleichung

$$Ax^2 + By^2 + Cz^2 = 0.$$