Eine neue Darstellung des biquadratischen Charakters

von

Josef Anton Gmeiner in Innsbruck.

Ist $m = a+bi$ eine ungerade complexe ganze Zahl, p deren Norm und $\alpha+\beta i$ eine beliebige zu m theilerfremde ganze Zahl; setzen wir ferner

$$\left[\frac{a\alpha+b\beta}{p}\right] = \mathrm{K}_1,\ \left[\frac{a\beta-b\alpha}{p}\right] = \mathrm{K}_2,\ \left\{\frac{a\alpha+b\beta}{p}\right\} = \Lambda_1 \text{ und } \left\{\frac{a\beta-b\alpha}{p}\right\} = \Lambda_2,$$

wobei allgemein $[A]$ die grösste in A enthaltene ganze Zahl und $\{A\}$ die nächste ganze Zahl von A bedeuten soll, und ist

$$\left.\begin{aligned} \alpha+\beta i &= (\mathrm{K}_1+\mathrm{K}_2 i)(a+bi)+(x+yi) \\ \text{und}\quad \alpha+\beta i &= (\Lambda_1+\Lambda_2 i)(a+bi)+(u+vi) \end{aligned}\right\} \tag{1}$$

so sind $x+yi$ und $u+vi$ die Zahlen, welche Gauss in seiner „theoria residuorum biquadraticorum" als simpliciter residuum minimum, den kurzweg kleinsten Rest, und residuum absolute minimum, den absolut kleinsten Rest der Zahl $\alpha+\beta i$ modulo m bezeichnet.

Setzt man

$$\xi = ax+by,\ \eta = ay-bx,\ \mu = au+bv \text{ und } \nu = av-bu,$$

so folgt aus der Definition der kurzweg und absolut kleinsten Reste unmittelbar

$$0 \leqq \xi \leqq p-1,\ 0 \leqq \eta \leqq p-1,\ -\frac{p-1}{2} \leqq \mu \leqq \frac{p-1}{2}$$

$$\text{und } -\frac{p-1}{2} \leqq \nu \leqq \frac{p-1}{2} \tag{2}$$

Aus den Gleichungen (1) folgt ferner

$x+yi \equiv u+vi$ (mod. m), also auch $ax+ayi \equiv au+avi$ (mod. m) und, da

$$ai \equiv b \text{ (mod. } m)$$

ist,

$$ax+by \equiv au+bv \text{ (mod. } m) \text{ und daher auch } \left(\text{mod. } \frac{p}{t}\right),$$

wo t den grössten gem. Theiler von a und b bezeichnet.

Es ist also

$$\xi \equiv \mu \left(\text{mod. } \frac{p}{t}\right). \tag{3}$$

Ebenso findet man aus

$$b(x+yi) \equiv b(u+vi) \text{ (mod. } m),$$

da

$$bi \equiv -a \text{ (mod. } m)$$

ist,

$$\eta \equiv \nu \left(\text{mod. } \frac{p}{t}\right). \tag{4}$$

Nehmen wir nun weiter an, dass in $m = a+bi$ a und b zu einander theilerfremd seien, so bestehen, wie Gauss bewiesen hat, zwischen den Grössen ξ und η folgende Beziehungen:

1. Es kann nicht eine der Grössen ξ und η Null sein, ohne dass auch die andere Null ist.

2. Es kann nicht $\xi = \eta$ sein.

3. Es kann nicht $\xi + \eta = p$ sein.

Aus diesen Relationen zwischen ξ und η und aus den Congruenzen (3) und (4) ergeben sich unmittelbar die folgenden zwischen den Zahlen μ und ν bestehenden Beziehungen:

1. „Es kann nicht eine der Grössen μ und ν Null sein, ohne dass zugleich auch die andere Null ist." Denn aus $\mu = 0$ würde der Reihe nach $\xi = 0$, $\eta = 0$, $\nu = 0$ folgen, und für $\nu = 0$ ergeben sich dieselben Gleichungen in umgekehrter Reihenfolge. Lässt man also den Rest Null ausser Acht, so kann man sagen, μ und ν können nur die Werthe $\frac{p-1}{2}$, $\frac{p-3}{2}$, ... 2, 1, −1, −2, ... $-\frac{p-1}{2}$ annehmen.

2. „Es kann nicht $\mu = \nu$ sein"; denn daraus würde $\xi = \eta$ folgen.

3. „Es kann nicht $\mu+\nu = 0$ sein"; denn daraus würde sich $\xi+\eta = p$ ergeben.

Diese Sätze lassen sich leicht auch direct beweisen.

Ist $\mu = au+bv = 0$, so ist $au = -bv$, also $a\nu = (a^2+b^2)v = pv$.

Da nun a zu p theilerfremd ist, so muss ν durch p theilbar und daher zufolge (2) $\nu = 0$ sein.

Wäre $\mu = \nu$, also $au+bv = av-bu$, so würde daraus

$$a^2(u-v)+ab(u+v) = p(u-v)+b(au+bv+av-bu) =$$
$$p(u-v)+b(\mu+\nu) = p(u-v)+2b\mu = 0$$

folgen. Demnach müsste μ durch p theilbar sein, was zufolge (2) nicht möglich ist.

Wäre $\mu+\nu = 0$, also $a(u+v)+b(v-u) = 0$, so müsste

$$a^2(u+v)+ab(v-u) = p(u+v)+b(\nu-\mu) = p(u+v)-2b\mu = 0$$

sein, was wieder die Theilbarkeit von durch p voraussetzen würde.

Bezüglich der Zahlen μ und ν besteht ferner noch der Satz:

„Wenn zwei Zahlen dasselbe μ, beziehungsweise dasselbe ν entspricht, so entspricht ihnen auch dasselbe ν, beziehungsweise μ, und sie sind daher einander modulo m congruent."

Beweis:

Aus $\mu = au+bv$ und $\nu = av-bu$ folgt unmittelbar $a\mu-b\nu = pu$.

Es ist daher

$$a\mu \equiv b\nu \pmod{p}. \tag{5}$$

Sind nun $\mu_1\nu_1$ und $\mu_2\nu_2$ je zwei zusammengehörige Werthe von und ν und ist $\mu_1 = \mu_2$, so folgt aus (5)

$$b\nu_1 \equiv b\nu_2 \pmod{p},$$

also, da b zu p theilerfremd ist,

$$\nu_1 \equiv \nu_2 \pmod{p},$$

und dies ist zufolge (2) nur möglich, wenn $\nu_1 = \nu_2$ ist.

Ebenso folgt aus der Annahme $\nu_1 = \nu_2$ die Gleichung $\mu_1 = \mu_2$.

Aus diesem Satze erkennen wir, dass, während $\alpha+\beta i$ ein vollständiges Restensystem modulo m durchläuft, die Zahlen

Aus den Gleichungen (1) folgt ferner

$x+yi \equiv u+vi$ (mod. m), also auch $ax+ayi \equiv au+avi$ (mod. m) und, da

$$ai \equiv b \text{ (mod. } m)$$

ist,

$$ax+by \equiv au+bv \text{ (mod. } m) \text{ und daher auch } \left(\text{mod. } \frac{p}{t}\right),$$

wo t den grössten gem. Theiler von a und b bezeichnet.

Es ist also

$$\xi \equiv \mu \left(\text{mod. } \frac{p}{t}\right). \tag{3}$$

Ebenso findet man aus

$$b(x+yi) \equiv b(u+vi) \text{ (mod. } m),$$

da

$$bi \equiv -a \text{ (mod. } m)$$

ist,

$$\eta \equiv \nu \left(\text{mod. } \frac{p}{t}\right). \tag{4}$$

Nehmen wir nun weiter an, dass in $m = a+bi$ a und b zu einander theilerfremd seien, so bestehen, wie Gauss bewiesen hat, zwischen den Grössen ξ und η folgende Beziehungen:

1. Es kann nicht eine der Grössen ξ und η Null sein, ohne dass auch die andere Null ist.

2. Es kann nicht $\xi = \eta$ sein.

3. Es kann nicht $\xi + \eta = p$ sein.

Aus diesen Relationen zwischen ξ und η und aus den Congruenzen (3) und (4) ergeben sich unmittelbar die folgenden zwischen den Zahlen μ und ν bestehenden Beziehungen:

1. „Es kann nicht eine der Grössen μ und ν Null sein, ohne dass zugleich auch die andere Null ist.“ Denn aus $\mu = 0$ würde der Reihe nach $\xi = 0$, $\eta = 0$, $\nu = 0$ folgen, und für $\nu = 0$ ergeben sich dieselben Gleichungen in umgekehrter Reihenfolge. Lässt man also den Rest Null ausser Acht, so kann man sagen, μ und ν können nur die Werthe $\frac{p-1}{2}, \frac{p-3}{2}, \ldots 2, 1, -1, -2, \ldots -\frac{p-1}{2}$ annehmen.

2. „Es kann nicht $\mu = \nu$ sein“; denn daraus würde $\xi = \eta$ folgen.

3. „Es kann nicht $\mu+\nu = 0$ sein"; denn daraus würde sich $\xi+\eta = p$ ergeben.

Diese Sätze lassen sich leicht auch direct beweisen.

Ist $\mu = au+bv = 0$, so ist $au = -bv$, also $a\nu = (a^2+b^2)v = pv$.

Da nun a zu p theilerfremd ist, so muss ν durch p theilbar und daher zufolge (2) $\nu = 0$ sein.

Wäre $\mu = \nu$, also $au+bv = av-bu$, so würde daraus

$$a^2(u-v)+ab(u+v) = p(u-v)+b(au+bv+av-bu) = \\ p(u-v)+b(\mu+\nu) = p(u-v)+2b\mu = 0$$

folgen. Demnach müsste μ durch p theilbar sein, was zufolge (2) nicht möglich ist.

Wäre $\mu+\nu = 0$, also $a(u+v)+b(v-u) = 0$, so müsste

$$a^2(u+v)+ab(v-u) = p(u+v)+b(\nu-\mu) = p(u+v)-2b\mu = 0$$

sein, was wieder die Theilbarkeit von durch p voraussetzen würde.

Bezüglich der Zahlen μ und ν besteht ferner noch der Satz:

„Wenn zwei Zahlen dasselbe μ, beziehungsweise dasselbe ν entspricht, so entspricht ihnen auch dasselbe ν, beziehungsweise μ, und sie sind daher einander modulo m congruent."

Beweis:

Aus $\mu = au+bv$ und $\nu = av-bu$ folgt unmittelbar $a\mu-b\nu = pu$.

Es ist daher

$$a\mu \equiv b\nu \pmod{p}. \tag{5}$$

Sind nun $\mu_1\nu_1$ und $\mu_2\nu_2$ je zwei zusammengehörige Werthe von μ und ν und ist $\mu_1 = \mu_2$, so folgt aus (5)

$$b\nu_1 \equiv b\nu_2 \pmod{p},$$

also, da b zu p theilerfremd ist,

$$\nu_1 \equiv \nu_2 \pmod{p},$$

und dies ist zufolge (2) nur möglich, wenn $\nu_1 = \nu_2$ ist.

Ebenso folgt aus der Annahme $\nu_1 = \nu_2$ die Gleichung $\mu_1 = \mu_2$.

Aus diesem Satze erkennen wir, dass, während $\alpha+\beta i$ ein vollständiges Restensystem modulo m durchläuft, die Zahlen und ν alle Werthe $-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots -2, -1, 1, 2, \ldots \frac{p-3}{2}$ $\frac{p-1}{2}$ annehmen müssen.

Wir wollen nun untersuchen, in welcher Beziehung die zu den einander associirten Zahlen $\alpha+\beta i$ und $i(\alpha+\beta i)$ gehörigen μ und ν modulo m zu einander stehen.

Es sei $\mu_1\nu_1$ das zu $\alpha+\beta i$ und $\mu_2\nu_2$ das zu $i(\alpha+\beta i)$ gehörige Werthepaar von μ und ν, dann ist

$$\mu_1 \equiv a\alpha+b\beta \text{ (mod. } p), \quad \nu_1 \equiv a\beta-b\alpha \text{ (mod. } p)$$
$$\mu_2 \equiv -a\beta+b\alpha \text{ (mod. } p) \text{ und } \nu_2 \equiv a\alpha+b\beta \text{ (mod. } p),$$

wie sich aus der zweiten der Gleichungen (1) leicht ergibt.

Es ist also

$$\mu_2 \equiv -\nu_1 \text{ (mod. } p) \text{ und } \nu_2 \equiv \mu_1 \text{ (mod. } p)$$

und daher $\mu_2 = -\nu_1$ und $\nu_2 = \mu_1$.

Nehmen wir die vier einander associirten Zahlen $(\alpha+\beta i)i^\varkappa$ $(\varkappa = 0, 1, 2, 3)$ und bezeichnen die ihnen entsprechenden Werthepaare von μ und ν mit und $\nu_\varkappa$, so ist demnach

$$\mu_2 = -\nu_1, \; \nu_2 = \mu_1, \; \mu_3 = -\nu_2 = -\mu_1, \; \nu_3 = \mu_2 = -\nu_1,$$
$$\mu_4 = -\nu_3 = \nu_1, \; \nu_4 = \mu_3 = -\mu_1.$$

Wir haben daher folgendes Schema:

		ν
$\alpha+\beta i$	μ_1	ν_1
$i(\alpha+\beta i)$	$-\nu_1$	μ_1
$i^2(\alpha+\beta i)$	$-\mu_1$	$-\nu_1$
$i^3(\alpha+\beta i)$	ν_1	$-\mu_1$

Dieses Schema sagt uns: Unter den vier associirten Zahlen gibt es immer eine, für welche $\mu > 0$ und $\nu > 0$, eine, für welche $\mu < 0$ und $\nu > 0$, eine, für die $\mu < 0$ und $\nu < 0$, und endlich eine, für die $\mu > 0$ und $\nu < 0$ ist. Es gibt also im ganzen Restensystem modulo m $\frac{p-1}{4}$ Zahlen, für welche $\mu > 0$ und $\nu > 0$, $\frac{p-1}{4}$ Zahlen, für welche $\mu < 0$ und $\nu > 0$ ist, u. s. w.

Wir können daher das vollständige Restensystem modulo m auch so in Viertelrestensysteme eintheilen, dass wir in das erste Viertelsystem jene Zahlen nehmen, für welche $\mu > 0$ und $\nu > 0$, in das zweite jene, für welche $\mu < 0$ und $\nu > 0$, in das dritte jene, für welche $\mu < 0$ und $\nu < 0$, in das vierte jene, für welche $\mu > 0$ und $\nu < 0$ ist. Dadurch kommt jede der associirten Zahlen in eine andere Gruppe, und zwar wenn $\alpha+\beta i$ der ersten Gruppe angehört, so gehören bei dieser Eintheilung die Zahlen $i(\alpha+\beta i)$, $i^2(\alpha+\beta i)$ und $i^3(\alpha+\beta i)$ der Reihe nach in die zweite, dritte und vierte Gruppe.

Wir haben also durch unsere Eintheilung das vollständige Restensystem modulo m regelrecht in Viertelrestensysteme zerlegt.

Aus diesen Betrachtungen folgt unter Berücksichtigung der Relationen (2), (3) und (4), dass, wenn $\alpha+\beta i$ zum ersten Viertelsysteme gehört, $\xi = \mu$ und $\eta = \nu$ sein muss. Ebenso erkennt man, dass $\mu = \xi - p$ und $\nu = \eta$ oder $\mu = \xi - p$ und $\nu = \eta - p$ oder $\mu = \xi$ und $\nu = \eta - p$ sein muss, je nachdem $\alpha+\beta i$ dem zweiten, dritten oder vierten Viertelsystem angehört.

Vergleichen wir nun die Grössen Λ_1 und K_1 einerseits und die Grössen Λ_2 und K_2 anderseits miteinander, so finden wir Folgendes:

α) Es gehöre $\alpha+\beta i$ dem ersten Viertelsystem an; dann ist $\mu = \xi$ und $\nu = \eta$, also $u+vi = x+yi$, folglich auch

$$\Lambda_1 = K_1 \text{ und } \Lambda_2 = K_2.$$

β) Gehört $\alpha+\beta i$ zum zweiten Viertelsystem, so ist $\mu = \xi - p$ und $\nu = \eta$, d. h.

$$ay - bx = av - bu,$$

$$by + ax = au + bv + p$$

und daraus ergibt sich $x = a+u$ und $y = b+v$, folglich ist nach (1)

$$(\Lambda_1 + \Lambda_2 i)m = (K_1 + K_2 i)m + m, \text{ also}$$

$$\Lambda_1 = K_1 + 1 \text{ und } \Lambda_2 = K_2.$$

γ) Gehört $\alpha+\beta i$ zum dritten Viertelsystem, so ist $\mu = \xi - p$ und $\nu = \eta - p$, d. h.

$$ay - bx = av - bu + p \text{ und } by + ax = au + bv + p$$

und demzufolge $x = u + a - b$ und $y = v + a + b$.

Wir erhalten somit

$$(\Lambda_1 + \Lambda_2 i)m = (\mathrm{K}_1 + \mathrm{K}_2 i)m + (1+i)m, \text{ mithin}$$
$$\Lambda_1 = \mathrm{K}_1 + 1 \text{ und } \Lambda_2 = \mathrm{K}_2 + 1.$$

δ) Ist endlich $\alpha+\beta i$ eine Zahl des vierten Viertelsystems, so ist $\mu = \xi$ und $\nu = \eta - p$, d. h.

$$ay - bx = av - bu + p \text{ und } by + ax = au + bv.$$

Aus diesen Gleichungen findet man $x = u - b$ und $y = v + a$. Es ist demnach im vorliegenden Falle

$$(\Lambda_1 + \Lambda_2 i)m = (\mathrm{K}_1 + \mathrm{K}_2 i)m + im, \text{ also}$$
$$\Lambda_1 = \mathrm{K}_1 \text{ und } \Lambda_2 = \mathrm{K}_2 + 1.$$

Es sei nun im Folgenden m eine zweigliedrige ungerade Primzahl, $u_r + v_r i$ ein beliebiger absolut kleinster Rest modulo m, k eine beliebige, zu m theilerfremde, reelle ganze Zahl, und wir setzen

$$\Lambda_{1,r} = \left\{ \frac{(au_r + bv_r)k}{p} \right\}, \quad \Lambda_{2,r} = \left\{ \frac{(av_r - bu_r)k}{p} \right\},$$

$$\mathrm{K}_{1,r} = \left[\frac{(au_r + bv_r)k}{p} \right], \quad \mathrm{K}_{2,r} = \left[\frac{(av_r - bu_r)k}{p} \right],$$

$$d_{1,r} = \Lambda_{1,r} - \mathrm{K}_{1,r} \text{ und } d_{2,r} = \Lambda_{2,r} - \mathrm{K}_{2,r};$$

dann ist

$$(u_r + v_r i)k \equiv (u_{\varkappa_r} + v_{\varkappa_r} i)\, i^{d_{1,r} + 2 d_{1,r} d_{2,r} + 3 d_{2,r}} \pmod{m}, \tag{6}$$

wobei $u_r + v_r i$ und $u_{\varkappa_r} + v_{\varkappa_r} i$ absolut kleinste Reste des ersten Viertelsystems sind.

Beweis:

α) Gehört $(u_r + v_r i)k$ dem ersten Viertelsystem an, so ist, wie wir gesehen haben, $\Lambda_{1,r} = \mathrm{K}_{1,r}$ und $\Lambda_{2,r} = \mathrm{K}_{2,r}$, also $d_{1,r} = d_{2,r} = 0$, somit, wenn wir der Kürze wegen noch

$$d_{1,r} + 2 d_{1,r} d_{2,r} + 3 d_{2,r} = D_r$$

setzen,

$$D_r = 0,$$

also die Formel (6) richtig.

β) Gehört $(u_r + v_r i)k$ dem zweiten Viertelsystem an, so ist $\Lambda_{1,r} = K_{1,r}+1$ und $\Lambda_{2,r} = K_{2,r}$, also $d_{1,r} = 1$ und $d_{2,r} = 0$, mithin

$$D_r = 1,$$

d. h. die Formel (6) ist auch für diesen Fall richtig.

γ) Gehört $(u_r + v_r i)k$ zum dritten Viertelsystem, so ist $\Lambda_{1,r} = K_{1,r}+1$ und $\Lambda_{2,r} = K_{2,r}+1$, also $d_{1,r} = d_{2,r} = 1$ und

$$D_r = 6 \equiv 2 \pmod{4};$$

es besteht also wieder die Congruenz (6).

δ) Gehört $(u_r + v_r i)k$ zum vierten Viertelsystem, so ist $\Lambda_{1,r} = K_{1,r}$ und $\Lambda_{2,r} = K_{2,r}+1$, $d_{1,r} = 0$ und $d_{2,r} = 1$, also

$$D_r = 3,$$

somit bleibt die Formel (6) auch in diesem Falle bestehen, womit die Allgemeingiltigkeit derselben bewiesen ist.

Bilden wir alle Producte, welche wir erhalten, indem wir k mit je einem Reste des ersten Viertelsystems multipliciren, stellen für jedes dieser Producte die Congruenz (6) auf und multipliciren alle diese Congruenzen miteinander, so bekommen wir

$$k^{\frac{p-1}{4}} \prod_{r=1}^{\frac{p-1}{4}} (u_r + v_r i) \equiv \prod_{r=1}^{\frac{p-1}{4}} (u_{\varkappa_r} + v_{\varkappa_r} i)\, i^{\sum_{r=1}^{\frac{p-1}{4}} D_r} \pmod{m}.$$

Nun ist bekanntlich das Product auf der rechten Seite dieser Congruenz mit dem Producte auf der linken Seite identisch und zu m theilerfremd. Es ist daher

$$k^{\frac{p-1}{4}} \equiv i^{\sum_{r=1}^{\frac{p-1}{4}} D_r} \pmod{m}. \tag{7}$$

Da

$$\Lambda_{1,r} = \left\{\frac{(au_r + bv_r)k}{p}\right\} = \left\{\frac{\mu_r k}{p}\right\}, \quad \Lambda_{2,r} = \left\{\frac{(av_r - bu_r)k}{p}\right\} = \left\{\frac{\nu_r k}{p}\right\}$$

und ebenso

$$K_{1,r} = \left[\frac{\mu_r k}{p}\right] \text{ und } K_{2,r} = \left[\frac{\nu_r k}{p}\right]$$

ist, so nimmt D_r die Gestalt an

$$D_r = d_{1,r} + 2 d_{1,r} d_{2,r} + 3 d_{2,r} =$$

$$= \left(\left\{\frac{\mu_r k}{p}\right\} - \left[\frac{\mu_r k}{p}\right] + 2\left(\left\{\frac{\mu_r k}{p}\right\} - \left[\frac{\mu_r k}{p}\right]\right)\left(\left\{\frac{\nu_r k}{p}\right\} - \left[\frac{\nu_r k}{p}\right]\right) + \right.$$
$$\left. + 3\left(\left\{\frac{\nu_r k}{p}\right\} - \left[\frac{\nu_r k}{p}\right]\right)\right).$$

Es ist demnach zufolge (7)

$$k^{\frac{p-1}{4}} \equiv i^{\sum\limits_{1}^{\frac{p-1}{4}}{}_r \left(\left\{\frac{\mu_r k}{p}\right\} - \left[\frac{\mu_r k}{p}\right] + 2\left(\left\{\frac{\mu_r k}{p}\right\} - \left[\frac{\mu_r k}{p}\right]\right)\left(\left\{\frac{\nu_r k}{p}\right\} - \left[\frac{\nu_r k}{p}\right]\right) + 3\left(\left\{\frac{\nu_r k}{p}\right\} - \left[\frac{\nu_r k}{p}\right]\right)\right)} \pmod{m}.$$

Diese Formel ist das Analogon zu der Formel

$$k^{\frac{p-1}{2}} \equiv (-1)^{\sum\limits_{1}^{\frac{p-1}{2}}{}_r \left(\left\{\frac{rk}{p}\right\} - \left[\frac{rk}{p}\right]\right)} \pmod{p}$$

in der Theorie der quadratischen Reste, worin p eine ungerade reelle Primzahl und k eine beliebige, zu p theilerfremde, reelle ganze Zahl bedeutet.

Durch die soeben entwickelte Formel kann der biquadratische Charakter einer jeden zu m theilerfremden Zahl $\alpha + \beta i$ dargestellt werden; denn bekanntlich gibt es stets eine reelle ganze Zahl k von der Beschaffenheit, dass

$$\alpha + \beta i \equiv k \pmod{m}$$

ist, wenn, wie wir hier vorausgesetzt haben, m eine zweigliedrige Primzahl bedeutet.