$$\sum_{j=1}^{\nu} a_{i(j)} w + b r' + q z = r d;$$

nach der im Hilfssatz 2 hervorgehobenen Eigenschaft von b ist also rd modulo q einer Summe von höchstens $\beta_2 \cdot \beta_2 + \beta_1$ Summanden $\pm a_i$ kongruent.

Bemerkung. Beschränkt man sich im Khintchineschen Satz auf den Fall, dass q eine *Primzahl* ist, so ist dieser Satz — und zwar mit $\delta = \frac{2}{\gamma^{n-1}}$ — eine unmittelbare Folge des folgenden Satzes vom Herrn Davenport [7]: „Ist q eine Primzahl, sind die Zahlen $a_1, \ldots, a_k$ — und ebenso die Zahlen $b_1, \ldots b_l$ — paarweise inkongruent modulo q, so stellen die Zahlen $a_i + b_j (1 \leqq i \leqq k, 1 \leqq j \leqq l)$ mindestens $\mathrm{Min}(k+l-1, q)$ verschiedene Restklassen modulo q dar". In der Tat: ist $\gamma^n q \leqq 2$, so hat jede Kongruenz

$$(13) \qquad \sum_{i=1}^{n} r_i x_i \equiv m \pmod q$$

eine Lösung mit

$$|x_i| < q = q^{\frac{n-1}{n}} q^{\frac{1}{n}} \leqq \frac{2^{\frac{n-1}{n}}}{\gamma^{n-1}} q^{\frac{1}{n}} < \delta q^{\frac{1}{n}}.$$

Ist aber $\gamma^n q > 2$, so beachte man, dass die Zahlen (9) mehr als $\gamma^n q > 2$ verschiedene Restklassen modulo q darstellen (also $\gamma \leqq 1$). Man wähle $c = \left[\frac{2}{\gamma^n}\right]$; dann ist

$$\gamma^n q + (c-1)(\gamma^n q - 1) > (c+1)\frac{\gamma^n}{2} q > q;$$

durch wiederholte Anwendung des Davenportschen Satzes bekommt man also folgendes Resultat: jedes m ist modulo q einer Summe von höchstens c Zahlen (9) kongruent; also hat (13) eine Lösung mit

$$|x_i| \leqq c \cdot \gamma q^{\frac{1}{n}} \leqq \delta q^{\frac{1}{n}}.$$

(Eingegangen am 1. Oktober 1936.)

[7]) H. Davenport: On the addition of residue classes, Journal of the London Mathematical Society 10 (1935), S. 30 — 32.

Eine Aufgabe aus der algebraischen Zahlentheorie.

Von

N. Tschebotaröw (Kasan).

(Meinem verehrten Lehrer Prof. Dr. A. Grawe zum 50. Jahr seiner wissenschaftlichen Tätigkeit gewidmet).

In einer meiner früheren Arbeiten [1]) habe ich die Existenzfrage von gewissen relativ Abelschen Zahlkörper auf das Existenzproblem der l-primären Primideale $\mathfrak{p}$ innerhalb eines gegebenen normalen algebraischen Zahlkörpers k zurückgeführt derart, dass das Potenzrestsymbol

$$(1) \qquad \left\{\frac{\Pi_2 \cdot \Pi_3 \ldots \Pi_\varkappa}{\mathfrak{p}}\right\}$$

einen vorgeschriebenen Wert hat, wobei $\mathfrak{p}_1 = \mathfrak{p}, \mathfrak{p}_2, \ldots, \mathfrak{p}_\varkappa$ die mit $\mathfrak{p}$ konjugierten Primideale und $\Pi_i = \mathfrak{p}_i \mathfrak{q}_i^l$ $(i = 1, 2, \ldots, k)$ die miteinander konjugierten ganzen Zahlen von k $[(\mathfrak{p}_1 \cdot \mathfrak{p}_2 \ldots \mathfrak{p}_\varkappa, \mathfrak{q}_i) = 1]$ bedeuten. Der Wert des Symbols (1) hängt wegen der Primärität von $\mathfrak{p}$ nicht von der Wahl der $\mathfrak{q}_i$ ab.

Diese Aufgabe schien mir mit Hilfe der heutigen Methoden der analytischen Zahlentheorie unauflösbar, da ich sie nicht auf die Frobeniussche Aufgabe über die Existenz von zu verschiedenen Substitutionen der Gruppe eines Zahlkörpers gehörenden Primidealen zurückführen

[1]) N. Tschebotaröw, Untersuchungen über relativ Abelsche Zahlkörper. Journ. für Math. 167 (1932), S. 98 — 121.

konnte. Nun ist es mir gelungen, das bei $l=2$ für alle quadratisch-imaginären Zählkörper $k(\sqrt{-m})$ darzutun, wo m eine ganze ungerade quadratfreie und in der Form x^2+y^2 darstellbare Zahl ist.

§ 1.

Im folgenden werden wir der Formeln bedienen, die die Legendreschen Symbole in irrationalen algebraischen Zahlkörpern durch Symbole im Körper der rationalen Zahlen ausdrücken lassen. Diese Formeln werden von Ph. Furtwängler[2]) für relativ normale Zahlkörper und von T. Takagi[3]) für den allgemeinen Fall hergeleitet.

Es bezeichne $\{\ldots\}$ das l-te Potenzrestsymbol im Körper K und $(\ldots)$ in seinem Unterkörper k, $N(\ldots)$ die Relativnorm von Zahlen und Idealen des Körpers K in bezug auf k. Dann gilt:

$$\left\{\frac{\alpha}{\mathfrak{P}}\right\}=\left(\frac{\alpha}{N(\mathfrak{P})}\right), \tag{2}$$

wobei α eine Zahl aus k und $\mathfrak{P}$ ein Ideal aus K bedeutet. Ferner gilt

$$\left\{\frac{A}{\mathfrak{b}}\right\}=\left(\frac{N(A)}{\mathfrak{b}}\right), \tag{3}$$

wobei A eine Zahl aus K und $\mathfrak{b}$ ein Ideal aus k bedeutet.

§ 2.

Es seien k der Körper der rationalen Zahlen und K ein quadratisch-imaginärer Zahlkörper: $K=k(\sqrt{-m})$, wobei m eine ganze positive ungerade quadratfreie Zahl ist. Wir nehmen ferner an, m sei in die Summe zweier Quadrate zerlegbar: $m=\xi^2+\eta^2$.

Das bedeutet, dass jeder Primfaktor q_i von m:

$$m=q_1\, q_2 \ldots q_s \tag{4}$$

der Kongruenz

$$q_i\equiv 1 \pmod 4 \qquad (i=1,2,\ldots s) \tag{5}$$

genügt. Die Basis von K kann in die Form $[1, \sqrt{-m}]$ gebracht werden.

Die Bedingung: die Zahl

$$p=N(a+b\sqrt{-m})=a^2+m\,b^2 \tag{6}$$

soll eine ungerade Primzahl sein, — zieht nach sich entweder

$$a\equiv 1 \pmod 2,\ b\equiv 0 \pmod 2, \tag{7}$$

oder

$$a\equiv 0 \pmod 2,\ b\equiv 1 \pmod 2. \tag{8}$$

Im ersten Falle kann das gesuchte Symbol $\left\{\frac{a-b\sqrt{-m}}{a+b\sqrt{-m}}\right\}$ vermöge (2) folgendermassen transformiert werden:

$$\left\{\frac{a-b\sqrt{-m}}{a+b\sqrt{-m}}\right\}=\left\{\frac{2a}{a+b\sqrt{-m}}\right\}=\left(\frac{2a}{a^2+m b^2}\right)= \tag{9}$$

$$=\left(\frac{2}{a^2+m b^2}\right)\left(\frac{m}{a}\right)=(-1)^{\frac{p-1}{4}}\cdot\left(\frac{a}{m}\right).$$

Das Jacobische Symbol $\left(\frac{a}{m}\right)$ lässt sich wegen (4) folgendermassen darstellen:

$$\left(\frac{a}{m}\right)=\left(\frac{a}{q_1}\right)\cdot\left(\frac{a}{q_2}\right)\ldots\left(\frac{a}{q_s}\right).$$

Jedes Symbol $\left(\frac{a}{q_i}\right)$ $(i=1,2,\ldots,s)$ hat den Wert $+1$ dann und nur dann, wenn die Kongruenz

$$\xi^2\equiv a \pmod{q_i} \tag{10}$$

rationale Lösungen besitzt. Da aber

$$p\equiv a^2 \pmod{q_i} \tag{11}$$

ist, so ist $\left(\frac{a}{q_i}\right)=+1$ dann und nur dann, wenn p ein *biquadratischer Rest* modulo q_i ist. Die Notwendigkeit dieser Bedingung ist klar. Ist andererseits $p\equiv\xi_1^4 \pmod{q_i}$, so gilt wegen (6) entweder $a\equiv\xi_1^2 \pmod{q_i}$, oder $a\equiv-\xi_1^2 \pmod{q_i}$. Beide Werte von a sind wegen

$$q_i\equiv 1 \pmod 4 \tag{12}$$

quadratische Reste modulo q_i. D. h. das Symbol $\left(\frac{a}{q_i}\right)$ hat den Wert $+1$.

---

[2]) Ph. Furtwängler, Über das Reciprocitätsgesetz der l-ten Potenzreste in algebraischen Zahlkörpern, wenn l eine ungerade Primzahl bedeutet. Math. Ann. 58 (1904), S. 24.

[3]) T. Takagi, Über das Reciprocitätsgesetz in einem beliebigen algebraischen Zahlkörper, Journ. of Coll. of Sc. Imp. Univ. Tôkyo 44 (1922), S. 10.

Sind wir imstande, die Kongruenzklasse modulo q_i, in welcher p liegen soll, nach unserer Willkür zu wählen, nehmen aber von vornherein an, p sei quadratischer Rest modulo q_i, so haben wir $\frac{p-1}{4}$ biquadratische Reste und $\frac{p-1}{4}$ Nichtreste zur Verfügung. Für die ersteren gilt $\left(\frac{a}{q_i}\right) = +1$, für die letzteren $\left(\frac{a}{q_i}\right) = -1$.

Fassen wir den Fall (8) ins Auge, so haben wir, indem wir

$$a = 2^{\lambda} \cdot a_1, \quad (a_1, 2) = 1$$

setzen:

$$\left\{\frac{a - b\sqrt{-m}}{a + b\sqrt{-m}}\right\} = \left(\frac{2a}{a^2 + mb^2}\right) = \left(\frac{2}{a^2 + mb^2}\right)^{\lambda+1} \left(\frac{m}{a_1}\right) = \tag{13}$$

$$= (-1)^{\frac{p-1}{4} \cdot (\lambda+1)} \cdot \left(\frac{a_1}{m}\right) = (-1)^{\frac{p-1}{4} \cdot (\lambda+1)} \cdot (-1)^{\frac{m-1}{4} \cdot \lambda} \left(\frac{a}{m}\right).$$

Nun wollen wir die Primzahl p einer weiteren Bedingung unterwerfen:

$$p \equiv m \pmod 8. \tag{14}$$

Dann erhalten die Ausdrücke (9) und (13) eine und dieselbe Gestalt:

$$\left\{\frac{a - b\sqrt{-m}}{a + b\sqrt{-m}}\right\} = (-1)^{\frac{m-1}{4}} \cdot \left(\frac{a}{m}\right), \tag{15}$$

so dass wir imstande sind, die Fälle (7) und (8) nicht zu unterscheiden. Also sehen wir, dass der Wert unseres Symbols $\left\{\frac{a - b\sqrt{-m}}{a + b\sqrt{-m}}\right\}$ vollständig bestimmt ist, sobald wir die Kongruenzklasse modulo $8m$ kennen, in welcher p liegt.

§ 3.

Einer besonderen Untersuchung bedarf der Fall, dass K der Gaussische Zahlkörper ist: $K = k(i)$. Dann können wir die Zahl $a + bi$ mit Hilfe der Einheiten ± 1, $\pm i$ so normieren, dass es gilt:

$$a > 0, \quad a \equiv 1 \pmod 2, \quad b \equiv 0 \pmod 2.$$

Sodann kann das gesuchte Symbol folgendermassen transformiert werden:

$$\left\{\frac{a - bi}{a + bi}\right\} = \left\{\frac{2a}{a + bi}\right\} = \left(\frac{2a}{a^2 + b^2}\right) = \left(\frac{2}{a^2 + b^2}\right)\left(\frac{a}{a^2 + b^2}\right) = (-1)^{\frac{p-1}{4}}. \tag{16}$$

Die Primäritätsbedingung $\left\{\frac{i}{a + bi}\right\} = 1$ verlangt aber, dass die Werte der Symbole $\left\{\frac{a - bi}{a + bi}\right\}$, $\left\{\frac{b + ai}{a + bi}\right\}$ einander gleich sind. Daraus folgt:

$$\left\{\frac{a - bi}{a + bi}\right\} = \left\{\frac{b + ai}{b - ai}\right\} = \left\{\frac{2b}{b - ai}\right\} = \left(\frac{2b}{a^2 + b^2}\right). \tag{17}$$

Es gilt also wegen (16): $\left(\frac{4ab}{a^2 + b^2}\right) = \left(\frac{2a}{a^2 + b^2}\right)\left(\frac{2b}{a^2 + b^2}\right) = 1$, woraus wir schliessen: $1 = \left(\frac{4ab}{a^2 + b^2}\right) = \left(\frac{2(a+b)^2 - 2(a^2 + b^2)}{a^2 + b^2}\right) = \left(\frac{2}{a^2 + b^2}\right)$.

Diese Bedingung kann auch folgendermassen geschrieben werden:

$$p \equiv 1 \pmod 8. \tag{18}$$

Ist diese Bedingung erfüllt, so ist der Wert des gesuchten Symbols $\left\{\frac{a - bi}{a + bi}\right\}$ wegen (16) gleich $+1$. Somit lässt unsere Aufgabe in diesem Fall eine *negative* Lösung zu.

§ 4.

Nun kehren wir uns wieder zum allgemeineren Fall des § 2 zurück. Um Primhauptideale $(a + b\sqrt{-m})$ zu finden, die der Bedingung

$$\left\{\frac{a - b\sqrt{-m}}{a + b\sqrt{-m}}\right\} = \varepsilon \tag{19}$$

genügen, brauchen wir, rationale Primzahlen $p = N(a + b\sqrt{-m})$ zu suchen, die folgenden Bedingungen unterworfen sind:

1) p sollen innerhalb $k(\sqrt{-m})$ in zwei verschiedene Primhauptideale zerfallen.

2) p sollen primär, d. h. von der Form $4k + 1$ sein. Sie sollen vielmehr der Kongruenz $p \equiv m \pmod 8$ genügen.

3) p sollen quadratische Reste modulo q_i $(i = 1, 2, \ldots, s)$ sein:

$$\left(\frac{p}{q_i}\right) = +1 \qquad (i = 1, 2, \ldots, s).$$

4) Bedeutet ε_i $+1$ oder -1, je nachdem p *biquadratischer* Rest bzw. Nichtrest modulo q_i ist (schon angenommen, dass 3) gilt), so soll

$$\varepsilon_1 \,.\, \varepsilon_2 \ldots \varepsilon_s = (-1)^{\frac{m-1}{4}} \varepsilon \tag{20}$$

sein, wobei ε eine vorgeschriebene Grösse $+1$ oder -1 ist.

Die Bedingung 1) kann mit Hilfe des Klassenkörpers folgendermassen umgeformt werden. Der Definition des Klassenkörpers zufolge [4]) ist p die Norm eines Hauptideals 1. Grades von K dann und nur dann, wenn p die Norm eines Ideals 1. Grades von $\mathfrak{K}$ ist, wobei $\mathfrak{K}$ den Klassenkörper von K bedeudet. Demnach ist die Bedingung 1) der folgenden Bedingung äquivalent:

1′) p sollen innerhalb $\mathfrak{K}$ zur identischen Permutation der Gruppe gehören.

Die Bedingungen 2), 3), 4) können ebenfalls auf ähnliche Weise formuliert werden. Dazu führen wir den Körper K_1 der $8m$-ten Einheitswurzeln ein. Dann sind die Bedingungen 2), 3), 4) zu folgender Bedingung äquivalent:

2′) p sollen innerhalb K_1 zu einer gewissen Permutationsklasse gehören.

Die Frage nach der Existenz von unendlich vielen Primzahlen, die innerhalb zwei verschiedener Körper $\mathfrak{K}$ und K_1 zu vorgeschriebenen Permutationsklassen gehören, hat eine positive oder negative Beantwortung [5]),

je nachdem die innerhalb beider Körper vorgegebenen Permutationen dieselbe Permutation innerhalb ihres Durchschnittes K_2 hervorrufen oder nicht.

Nun ist K_1 und also K_2 absolut Abelsch. Andereseits ist der grösste absolut Abelsche Teilklassenkörper des quadratischen Körpers $K = k(\sqrt{-m})$ der Körper $k(i, \sqrt{-q_1}, \sqrt{-q_2}, \ldots, \sqrt{-q_s})$ [6]). Da dieser Körper wirklich in K_1 enthalten ist, so ist

$$K_2 = k(i, \sqrt{-q_1}, \sqrt{-q_2}, \ldots, \sqrt{-q_s}). \tag{21}$$

[4]) Vgl. H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil I: Klassenkörpertheorie. Jber. D. M. V. 35 (1926), S. 4, Definition 1⁰.

[5]) Vgl. N. Tschebotareff, Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, die zu einer gegebenen Substitutionsklasse gehören. Math. Ann. 95 (1925), S. 213.

[6]) Vgl. N. Tschebotaröw, Zur Gruppentheorie des Klassenkörpers. Journ. für Math. 161 (1929), S. 193, Beispiel.

Der identischen Permutation in $\mathfrak{K}$ entpricht offenbar die identische Permutation in K_2. Es bleibt also, zu beweisen, dass auch die Permutation in K_2, die durch die mittels der Bedingungen 2, 3), 4) aufgestellten Permutation in K_1 hervorgerufen wird, die identische Permutation ist. Nun besteht aber die Bedingung dafür, dass p im Körper K_2 in lauter Primideale 1. Grades zerfällt, in der Befriedigung der Bedingungen

$$\left(\frac{-1}{p}\right) = +1, \left(\frac{q_1}{p}\right) = +1, \left(\frac{q_2}{p}\right) = +1, \ldots, \left(\frac{q_s}{p}\right) = +1. \tag{22}$$

Diese Bedingungen, nur die erste ausgenommen, fallen wegen das Legendreschen Reziprozitätsgesetzes mit der Bedingung 3) zusammen. Die erste der Bedingung (22) ist in der Bedingung 2) enthalten. Somit ist die Existenz der gesuchten Primzahlen bewiesen.

§ 5.

Es sei mir gestattet, auf die mit der Lösung unserer Aufgabe in anderen Fällen verbundenen Schwierigkeit hinzuweisen. Wir betrachten sämtliche Typen von quadratisch-imaginären Zahlkörper und führen für jeden Typ ähnliche Überlegung aus, wie wir zur Herleitung der Formeln (9), (13) angewendet haben.

I. $K = k(\sqrt{-m})$, $m \equiv 1 \pmod 4$. Die Basis ist $[1, \sqrt{-m}]$.

Die Formeln (9) und (13) bleiben unverändert bestehen:

$$\left\{\frac{a - b\sqrt{-m}}{a + b\sqrt{-m}}\right\} = (-1)^{\frac{p-1}{4}} \left(\frac{a}{m}\right) \quad [a \equiv 1 \pmod 2,\ b \equiv 0 \pmod 2]; \tag{23}$$

$$\left\{\frac{a - b\sqrt{-m}}{a + b\sqrt{-m}}\right\} = (-1)^{\frac{p-1}{4}(\lambda+1)} \cdot (-1)^{\frac{m-1}{4}\cdot\lambda} \left(\frac{a}{m}\right) \tag{24}$$

$$[b \equiv 1 \pmod 2,\ a = 2 \cdot a_1,\ (a_1, 2) = 1].$$

Wir müssen aber hier annehmen, m enthalte Primfaktoren vom Typ $4k+3$. Es sei q_1 einer solcher Primfaktoren. Dann ist $\left(\frac{a}{q_1}\right) = -\left(\frac{-a}{q_1}\right)$, so dass die Normierung $a > 0$ hier wesentlich ist. Andererseits hat die Kongruenz $\xi^4 \equiv p \pmod{q_1}$ bei $q_1 \equiv 3 \pmod 4$ stets zwei und nur zwei rationale Lösungen. Wir haben kein Mittel zur Entscheidung, ob die Kongruenz $\xi^2 \equiv a \pmod{q_1}$, $a > 0$ rationale Lösungen hat oder nicht.

Man kann die Formel (23) auch folgendermassen schreiben:

$$(25)\qquad \left\{\frac{a-b\sqrt{-m}}{a+b\sqrt{-m}}\right\}^{\prime\prime}=(-1)^{\frac{p-1}{4}}\prod_{i=1}^{s}(-1)^{\frac{a-1}{2}\cdot\frac{q_i-1}{2}}\cdot\left(\frac{a}{q_i}\right).$$

Hier hängt jeder Faktor $(-1)^{\frac{a-1}{2}\cdot\frac{q_i-1}{2}}\left(\frac{a}{q_i}\right)$ $(i=1,2,\ldots,s)$ von der Wahl des Verzeichens bei a nicht ab. Er hängt aber vom Verhalten der Zahl a modulo 4 ab, welches durch keine Kongruenzeigenschaft der Zahl p charakterisiert werden kann.

II. $K=k(\sqrt{-m})$, $m\equiv 3 \pmod 4$. Die Basis ist $\left[1,\ \frac{1+\sqrt{-m}}{2}\right]$. Die ganzen ungeraden Zahlen des Körpers K können also entweder in der Form

$$(26)\qquad \frac{a}{2}+\frac{b}{2}\sqrt{-m}$$

dargestellt werden, wobei $a\equiv 1 \pmod 2$, $b\equiv 1 \pmod 2$ gilt, oder in der Form $a+b\sqrt{-m}$, wobei entweder

$$(27)\qquad a\equiv 1 \pmod 2,\ b\equiv 0 \pmod 2$$

oder

$$(28)\qquad a\equiv 0 \pmod 2,\ b\equiv 1 \pmod 2$$

gilt. Im Falle (26) ist

$$\left\{\frac{\frac{a}{2}-\frac{b}{2}\sqrt{-m}}{\frac{a}{2}+\frac{b}{2}\sqrt{-m}}\right\}=\left\{\frac{a}{\frac{a}{2}+\frac{b}{2}\sqrt{-m}}\right\}=\left(\frac{a}{(a^2+mb^2):4}\right)=$$

$$=\left(\frac{(a^2+mb^2):4}{a}\right)=\left(\frac{a^2+mb^2}{a}\right)=\left(\frac{m}{a}\right)=(-1)^{\frac{a-1}{2}}\left(\frac{a}{m}\right)=$$

$$=\prod_{i=1}^{s}(-1)^{\frac{a-1}{2}\cdot\frac{q_i-1}{2}}\left(\frac{a}{q_i}\right).$$

Hier bewahren ihre Gültigkeit alle Bemerkungen zum Fall I.

Analog erhalten wir im Falle (27):

$$\left\{\frac{a-b\sqrt{-m}}{a+b\sqrt{-m}}\right\}=\left\{\frac{2a}{a+b\sqrt{-m}}\right\}=\left(\frac{2a}{a^2+mb^2}\right)=\left(\frac{2}{a^2+mb^2}\right)\left(\frac{m}{a}\right)=$$

$$=(-1)^{\frac{p-1}{4}}\cdot(-1)^{\frac{a-1}{2}}\left(\frac{a}{m}\right)=(-1)^{\frac{p-1}{4}}\prod_{i=1}^{s}(-1)^{\frac{a-1}{2}\cdot\frac{q_i-1}{2}}\left(\frac{a}{q_i}\right).$$

Im Falle (28) ist die Zahl p nicht primär.

III. Der Fall $K=k(\sqrt{-3})$ unterscheidet sich vom Fall II dadurch, dass der Körper $k(\sqrt{-3})$ nicht-triviale Einheiten

$$\varepsilon=\frac{-1+\sqrt{-3}}{2},\quad \varepsilon^2=\frac{-1-\sqrt{-3}}{2}$$

enthält. Man kann erwarten, dass hier die Primäritätsbedingung schärfer ist. Das ist aber nicht der Fall, da $\left\{\frac{\varepsilon}{\omega}\right\}=\left\{\frac{\varepsilon^2}{\omega}\right\}^2=+1$ gilt, wobei ω eine Primzahl des Körpers $k(\sqrt{-3})$ bedeutet.

IV. Der Fall $K=k(\sqrt{-2m})$, $m\equiv 1 \pmod{2}$. Die Basis ist $[1,\sqrt{-2m}]$. Es gilt: $a\equiv 1$, $b\equiv 0 \pmod 2$, da die Primäritätsbedingung

$$\left\{\frac{-1}{a+b\sqrt{-2m}}\right\}=\left(\frac{-1}{a^2+2mb^2}\right)=1$$

verlangt: $a^2+2mb^2\equiv 1 \pmod 4$. Daraus folgt: $p=a^2+2mb^2\equiv 1 \pmod 8$

Es gilt:

$$\left\{\frac{a-b\sqrt{-2m}}{a+b\sqrt{-2m}}\right\}=\left(\frac{2a}{a^2+2mb^2}\right)=\left(\frac{a^2+2mb^2}{a}\right)=\left(\frac{2}{a}\right)\left(\frac{m}{a}\right)=$$

$$=(-1)^{\frac{a^2-1}{8}}\cdot(-1)^{\frac{a-1}{2}\cdot\frac{m-1}{2}}\left(\frac{a}{m}\right).$$

Um diese Fälle zu erledigen, muss man die Dichtigkeiten der Primzahlen vom Typus $a+b\sqrt{-m}$ bestimmen, die den Bedingungen $a>0$, $a\equiv 1 \pmod 4$ genügen. Dazu dient folgende verallgemeinerte L-Reihe:

$$L(s)=\sum_{a,b}\frac{a+b\sqrt{-m}}{(a^2+mb^2)^s},$$

wobei a alle (positive und negative) ganzen Zahlen vom Typ $4k+1$ und b alle (bzw. alle geraden) ganzen Zahlen durchläuft, je nach Typ des Körpers $k(\sqrt{-m})$. Das werde ich in einer zukünftigen Arbeit dartun.

(Eingegangen am 25. Oktober 1936.)