§ 7 Dirichlet'sche Zahlkörper

Sei $K = \mathbb{Q}(i)$ und $R = \mathbb{Z}[i]$; R hat mit dem Ring $\mathbb{Z}$ viele Eigenschaften gemein, von denen wir hier einige aufzählen wollen. Dabei werden wir Elemente aus R mit kleinen (a, b, p, q), ganze rationale Zahlen dagegen mit großen (A, B, P, Q usw.) Buchstaben bezeichnen. Unter dem Begriff "rationale Primzahl" wollen wir immer eine natürliche Zahl verstehen. Weiter sei N immer die Norm von K nach $\mathbb{Q}$.

1. Die Einheitengruppe $R^\times$ ist endlich: $R^\times = \{ \pm i, \pm 1\}$;

2. R ist ZPE-Ring;

3. Jedes prime $p \in R$ ist zu einer der folgenden Zahlen assoziiert:
   a) $q = 1+i$, $N(q) = 2$,
   b) $p = A+Bi$, $A-1 \equiv B \equiv 0 \bmod 2$, $N(p) = A^2+B^2 = P$, wo $P \equiv 1 \bmod 4$ rationale Primzahl ist,
   c) $q = Q$, wo $Q \equiv 3 \bmod 4$ rationale Primzahl ist:

4. Ist $a \in R$, so gelten die Kongruenzen
   $a^2 \equiv 0 \bmod 4 \Leftrightarrow a \equiv 0 \bmod 2$
   $a^2 \equiv 2i \bmod 4 \Leftrightarrow a \equiv 1+i \bmod 2$
   $a^2 \equiv 1 \bmod 4 \Leftrightarrow a \equiv 1 \bmod 2$
   $a^2 \equiv 3 \bmod 4 \Leftrightarrow a \equiv i \bmod 2$;

5. Ist $p \in R$ prim und $(a,p) \neq 1$ für ein $a \in R$, dann gilt $a^{Np-1} \equiv 1 \bmod p$.

Der "kleine Fermat" in 5. gibt uns die Möglichkeit, in R ein quadratisches Restsymbol zu definieren: dazu seien $a,p \in R$, p prim, $Np \equiv 1 \bmod 2$ und $(a,p)=1$. Dann setzen wir $[a/p] = \pm 1$, wobei das Vorzeichen mit demjenigen in $a^{(Np-1)/2} \equiv \pm 1 \bmod p$ übereinstimmt. Dieses Restsymbol läßt sich in Analogie zum Jacobi-Symbol auch auf zusammengesetzte Nenner verallgemeinern; damit gilt dann

6. Das quadratische Reziprozitätsgesetz in $\mathbb{Z}[i]$: Für $a,b \in R$ mit $a \equiv b \equiv 1 \bmod 2$ gilt $[\frac{a}{b}] = [\frac{b}{a}]$. Weiter gelten mit $a = A+Bi$ und $Q = A+B$ die Ergänzungssätze $[\frac{i}{a}] = (-1)^{B/2}$ und $[\frac{1+i}{a}] = (\frac{2}{Q})$. Ist außerdem $b = C+Di$ prim und $D \neq 0$, so läßt sich mittels $[\frac{a}{b}] = (\frac{AC+BD}{P})$, $P = N(b) = C^2+D^2$ das Restsymbol (a/b) auf ein Legendre-Symbol zurückführen; diese Identität ermöglicht es auch, das QRG in R aus demjenigen in $\mathbb{Z}$ herzuleiten.

Auch die quadratischen Erweiterungen von K verhalten sich weitgehend wie die reellquadratischen Erweiterungen von $\mathbb{Q}$:

7. Sei $L = K(\sqrt{m})$, $m \in R$ quadratfrei, $S = O_L$ der Ring ganzer Zahlen in L; dann hat S die GHB $\{1, \beta\}$ über R, sowie die Relativdiskriminante d:

   I. $m \equiv 1 \mod 4$: $\beta = (1+\sqrt{m})/2$, $d = m$;

   II. $m \equiv \pm 1+2i \mod 4$: $\beta = (1+\sqrt{m})/(1+i)$, $d = 2im$;

   III. $m \equiv i \mod 2$ oder $m \equiv 0 \mod (1+i)$: $= \sqrt{m}$, $d = 4m$.

Ist $\alpha = r+s\sqrt{m}$ für $r,s \in K$, so heißt $\alpha' = r-s\sqrt{m}$ die Konjugierte von α : damit ist die Relativdiskriminante durch $d = (\alpha - \alpha')^2$ gegeben, wobei (auch im Folgenden) zu beachten ist, daß d nur bis auf einen Faktor ± 1 definiert ist. Allerdings hat dieser Faktor keinen Einfluß auf das Restsymbol $[\frac{d}{p}]$ oder die Erweiterung $K(\sqrt{d})$, weil ± 1 Quadrat ist. Schließlich errechnet sich die Absolutdiskriminante von L aus d durch $\operatorname{disc} L/\mathbb{Q} = 16N(d)$.

Nach 7. gilt für die Relativdiskriminante d quadratischer Erweiterungen von K die Kongruenz $d \equiv 0 \mod 2$ oder $d \equiv 1 \mod 4$; in der Tat gilt dies für Erweiterungen beliebigen Grades: wäre z.B. für die Relativdiskriminante d einer Erweiterung L/K $d \equiv \pm i \mod 4$, so wäre L/K sicher nicht galoisch (weil d kein Quadrat in K ist). Weiter ist $(1+i)$ in L/K unverzweigt, und folglich gilt dasselbe auch für den normalen Abschluß M/K. Dieser normale Abschluß M enthält aber den quadratischen Teilkörper $L(\sqrt{d})$, und wir sehen, daß $(1+i)$ auch in $L(\sqrt{d})$ unverzweigt ist. Nach dem Zerlegungsgesetz in relativquadratischen Erweiterungen (sh. Hilbert) muß dann die Kongruenz $x^2 \equiv d \mod 4$ in K lösbar sein, was wegen $d \equiv \pm i \mod 4$ aber nicht der Fall ist.

Derselbe Beweis funktioniert offensichtlich auch für den Fall $d \equiv \pm 1+2i \mod 4$. Ist schließlich $d \equiv 0 \mod (1+i)$, so ist $(1+i)$ in L/K verzweigt; bezeichnet $e = e(L/K)$ den Verzweigungsindex, so ist entweder $e=2$ oder $e \geq 3$, und in beiden Fällen folgt nach bekannten Sätzen (Stichwort: wilde Verzweigung) $(1+i)^2 \mid d$.

Um das Zerlegungsgesetz in L durch das Restsymbol $[\frac{d}{p}]$ beschreiben zu können, erweitern wir es analog zum Kronecker- Symbol und setzen für $p=1+i$

$$(d/p) = \begin{cases} +1, \text{ falls } d \equiv 1 \mod p^5 \\ -1, \text{ falls } d \equiv 5 \mod p^5 \end{cases}.$$

Damit gilt dann

8. Sei $p \in R$ prim, L/K quadratische Erweiterung von K mit Relativdiskriminante d; dann ist im Falle

   $[\frac{d}{p}] = +1$: $(p) = P_1P_2$ für zwei verschiedene Primideale P_1P_2 in S

   $[\frac{d}{p}] = -1$: $(p) = (p)$ bleibt prim;

   $[\frac{d}{p}] = 0$: $(p) = P^2$ verzweigt in L/K.

Aus der Tatsache, daß L totalkomplex ist, folgt erstens $N_{L/\mathbf{Q}}(\alpha) \geq 0$ für alle $\alpha \in L$, und zweitens nach dem Dirichletschen Einheitensatz

9. Jede Einheit $e \in S^\times$ läßt sich in der Form $e = \zeta u^k$ schreiben, wo ζ eine Einheitswurzel und u die FE von L ist. Dabei ist $\zeta = \zeta_8$, falls $L = K(\sqrt{i}) = \mathbf{Q}(i,\sqrt{2})$ ist; $\zeta = \zeta_{12}$, falls $L = K(\sqrt{-3})$ ist; $\zeta = \zeta_4 = i$ sonst.

Während man sich im Falle reellquadratischer Zahlkörper dafür interessiert, ob die Norm der FR gleich $+1$ oder gleich -1 ist, lautet die entsprechende Frage hier, ob $N_{L/K}(u) = \pm 1$ oder gleich $\pm i$ ist, und auch die Antworten sind weitgehend analog.

Die bisher aufgezählten Eigenschaften Dirichlet'scher Zahlkörper (damit werden die quadratischen Erweiterungen von K bezeichnet) sind klassisch und finden sich bereits bei Dirichlet und Hilbert. Mit ganz elementaren Methoden lassen sich aber auch hier weitergehende Ergebnisse erzielen.

Unser erstes Resultat betrifft die Parität der Klassenzahl von L; damit hat sich bisher nur Popovic (1958) befaßt; dieser zeigte, daß die Klassenzahl h=h(L) nur dann ungerade sein kann, wenn die Relativdiskriminante d prim ist oder $d \equiv \pm 1 \bmod 4$ gilt und d genau zwei Primteiler besitzt (übrigens sind die in der Besprechung dieser Arbeit (Reviews in number theory 1940 - 1972, R 16-33) angegebenen Behauptungen nicht richtig). Dieses Ergebnis läßt sich jedoch noch verschärfen, und dazu brauchen wir

(7.1) Sei $p \equiv \pm 1 \bmod 4$ prim in R; dann gibt es $a,b \in R$ mit $p = a^2 + ib^2$, $a \equiv 1 \bmod (1+i)$.

Bew.: Sei $L = K(\sqrt{i}) = \mathbf{Q}(i,\sqrt{2})$; L ist nach § 1 (oder auch § 5) normeuklidisch und hat damit Klassenzahl 1. Wegen $[\frac{i}{p}] = +1$ ist p in S zerlegt, folglich gibt es ein $\pi \in S$ mit $N_{L/K}(\pi) = \zeta p$, wo ζ eine Einheit in R ist (also $\zeta = \pm i, \pm 1$). Weil $\{1, i\}$ eine GHB von S über R ist, dürfen wir $\pi = a + b\sqrt{i}$ für gewisse $a,b \in R$ schreiben und finden $\zeta p = a^2 + ib^2$. Division durch ζ liefert nun die Behauptung.

Bem.: Das Analogon in $\mathbf{Z}$ ist die Darstellbarkeit von primen $P \equiv 1 \bmod 4$ als Summe zweier Quadrate; auch im Beweis von (7.2), der im reellquadratischen Fall auf Redei (1960) zurückgeht, übernimmt $p = a^2 + ib^2$ die Rolle vom $P = a^2 + b^2$ in Redeis Beweis.

(7.2) Sei $L = K(\sqrt{m})$, $m \in R$ quadratfrei. Ist dann $h(L) \equiv 1 \bmod 2$, dann kommen nur folgende Möglichkeiten in Betracht:

i) $m = i$

ii) $m = p$, $p \in R$ prim, $p \not\equiv \pm i \bmod 4$

iii) $m = pq \equiv \pm 1 \bmod 4$ für prime $p,q \in R$, wobei entweder $p,q \equiv \pm 1 + 2i \bmod 4$ oder $p = 1 \pm i$, $q \equiv \pm 1 + 2i \bmod 4$ ist.

Bew.: Sei d die Relativdiskriminante von L/K, wie sie in 7. definiert wurde. Da d (nach 7.) keine Einheit ist, gibt es prime $p \in R$ mit p|d. Nach dem Zerlegungsgesetz gilt $(p) = P^2$ für jedes solche P, wobei P ein Primideal in S über p ist. Da L nach Voraussetzung ungerade Klassenzahl hat, muß mit P^2 auch P ein Hauptideal sein, und es gibt ein $\pi \in S$, sowie eine Einheit $e \in S^\times$ mit $pe = \pi^2$, d.h. mit $\sqrt{pe} \in S$ (diese Einheit e hängt natürlich von dem jeweiligen p ab, das man gerade betrachtet).

Indem wir e gegebenenfalls mit einer geeigneten Potenz der Fundamentaleinheit u multiplizieren, dürfen wir uns auf die Möglichkeiten $e=\zeta$ und $e=\zeta u$ beschränken, wobei ζ eine 4. Einheitswurzel ist.

Ist nun $e=\zeta$ für irgendein p mit p|d, so folgt $\sqrt{\zeta p} \in S \setminus R$, und es muß $L = K(\sqrt{ep})$, also m=ep, sein: somit liegt Fall i) oder Fall ii) vor. Sei also $m \neq i$ und $e=\zeta u$ für alle p|d (wobei ζ, wie schon bemerkt, von p abhängt und nicht für jedes p gleich zu sein braucht). Dann folgt

I. $N_{L/K}(u) = 1$ (und nicht = i): mit pe ist nämlich auch pe' ein Quadrat in S, d.h. es gilt $\sqrt{pe} \cdot \sqrt{pe'} = p\sqrt{ee'} \in S$; wegen $m \neq i$ liegt $\sqrt{i}$ nicht in S, folglich muß $ee' = \pm uu' = \pm 1$ sein.

II. d hat maximal zwei Primteiler: ist nämlich p|d und q|d für prime, nicht assoziierte $p,q \in R$, so folgt mit $e_1 = \zeta_1 u$ und $e_2 = \zeta_2 u$: $\sqrt{pe_1} \cdot \sqrt{qe_2} = u\sqrt{pq\zeta_1\zeta_2} \in S$, und wir sehen $m \rightsquigarrow pq$. Sind außerdem p und q von $1 \pm i$ verschieden, so muß die Kongruenz $m \equiv \pm 1 \bmod 4$ gelten, da sonst außer p und q wegen 7. auch $1+i$ ein Teiler von d wäre.

Jetzt müssen wir noch folgende Möglichkeiten ausschließen (an dieser Stelle gehen wir über Popovic's Ergebnisse hinaus):

a) $m = pq$, $p = 1 \pm i$, $q \equiv \pm 1, \pm i \bmod 4$: (im Falle $q \equiv 2 \pm i \bmod 4$ ersetzen wir $p = 1+i$ durch $p = 1-i$, sodaß wir diesen Fall nicht extra behandeln müssen). Nach (7.1) existieren $a,b \in R$ mit $m = pq = a^2+ib^2$ und $a \equiv b \equiv 1 \bmod 1+i$. Wir setzen nun $\pi = a+\sqrt{m}$ und $\rho = (b, \pi)$; dabei ist π natürlich nur bis auf eine Einheit in S bestimmt. Wir sehen nun

$(\pi, \pi') = 1$: ein gemeinsamer Teiler σ von π und π' würde nämlich auch $\pi+\pi' = 2a$ und $\pi-\pi' = 2\sqrt{m}$ teilen; wegen (a,m)=1 ist aber erst recht $(a,\sqrt{m})=1$, sodaß σ Teiler von (2) sein müßte. Daraus folgt aber $(1+i) \mid N_{L/K}(\pi) = a^2-m = ib^2$ im Widerspruch zu $b \equiv 1 \bmod 1+i$.

ρ^2/π ist eine Einheit: dies folgt aus $(\rho^2) = (b,\pi)^2 = (b^2, b\pi, \pi^2) = (\pi\pi', b\pi, \pi^2) = \pi(\pi', b, \pi) = (\pi)$.

Nun ist $N_{L/K}(\rho) = \zeta b$ für eine 4. Einheitswurzel ζ, also $N_{L/K}(\rho)^2 = \pm b^2$, und weiter haben wir oben schon gesehen, daß $N_{L/K}(\pi) = ib^2$ gilt. Also hat die Einheit ρ^2/π die Norm $N_{L/K}(\rho^2/\pi) = \pm b^2/ib^2 = \pm i$ im Widerspruch zu I.

b) $m = pq \equiv 1 \bmod 4$, $p \equiv q \equiv 1 \bmod 4$: wie in a) ist auch hier $m = a^2+ib^2$; jedoch gilt nun $a-1 \equiv b \equiv 0 \bmod 2$. Wir setzen $\pi = (a+\sqrt{m})/2$, $\rho = (\pi, b/2)$ und schließen wie oben, daß ρ^2/π Einheit mit Norm $\pm i$ ist.

c) $m = p$, $p \equiv \pm i \bmod 4$: wir werden zeigen, daß $M = L(\sqrt{i})$ eine unverzweigte, quadratische (und damit abelsche) Erweiterung von L ist; nach der Klassenkörpertheorie (oder Hilberts Satz 94) muß dann die Klassenzahl von L gerade sein.
Da L totalkomplex ist, genügt es, endliche Primstellen zu betrachten. Weil i Einheit ist, können in M/L höchstens Primideale über (2) verzweigen. Wäre dies der Fall, müßte (2) in M rein verzweigt sein. Mit $F = \mathbb{Q}(\zeta_8)$ läßt sich aber $M = F(\sqrt{m})$ schreiben, und nach dem Zerlegungsgesetz für relativquadratische Erweiterungen (Hilbert) sind die Primideale über (2) in M/F unverzweigt (man beachte die Kongruenz $m \equiv i \equiv \sqrt{i}^2 \bmod 4$ in F).

Bem.: Es wäre wünschenswert, auch für den Fall c) einen Beweis zu haben, der ohne Klassenkörpertheorie auskommt.

Es ist interessant festzustellen, daß sich die Analogie der Dirichletschen zu quadratischen Zahlkörpern weiter fortsetzt: ganz genauso wie Cohn (1962) läßt sich nämlich nun zeigen:

- Sei $m = p \equiv \pm 1 \bmod 4$ prim und $L = K(\sqrt{m})$; dann gibt es eine Einheit $u \in S$ mit $N_{L/K}(u) = i$, und L hat ungerade Klassenzahl.
- Seien $p,q \equiv \pm 1+2i \bmod 4$ prim und nicht assoziiert, $m = pq$, $L = K(\sqrt{m})$; schreibt man $pS = P^2$, $qS = Q^2$ für Primideale P,Q in S, dann sind P und Q Hauptideale. Weiter gibt es $x,y \in R$ mit $4\zeta = px^2 + qy^2$, wo ζ eine 4. Einheitswurzel ist.

Genau wie bei Cohn kann man aus diesen beiden Tatsachen einen Beweis des QRG in R herleiten.

Wir wenden uns nun der Frage zu, welche Dirichletschen Zahlkörper normeuklidisch sind. Diese Frage läßt sich wie im reellquadratischen Fall dann am einfachsten behandeln, wenn die Relativdiskriminante durch eine hohe Potenz von 2 teilbar ist:

(7.3) Ist die Relativdiskriminante d von L/K durch 4 teilbar, dann ist L genau dann normeuklidisch, wenn $m=i$ oder $m=1+i$ gilt.

Zum Beweis verwenden wir

(7.4) Ist die Relativdiskriminante d von L/K durch 4 teilbar, die Klassenzahl h von L ungerade und $m \notin \{ i, 1 \pm i \}$, so gilt für die FE u die Kongruenz $u \equiv 1 \bmod (1+i)$.

Bew.: Da das Ideal $(1+i)$ in L/K verzweigt, gibt es ein Primideal 2_1 der Absolutnorm 2 in L. Da L ungerade Klassenzahl haben soll, ist 2_1 ein Hauptideal, d.h. es gibt ein $\pi \in S$ mit $(\pi)^2 = (1+i)$. Wegen $d \equiv 0 \bmod 4$ ist $\{1, \sqrt{m}\}$ eine GHB über R, sodaß wir $\pi = a+b\sqrt{m}$ für gewisse $a,b \in R$ schreiben können. Also ist $(a+b\sqrt{m}) = (1+i)e$ für eine Einheit $e \in S$. Nach dem Einheitensatz ist $e = \zeta u^k$ (ζ ist eine 4. Einheitswurzel, da L wegen $m \neq i$ keine 8., wegen $m \neq -3$ keine 12. Einheitswurzeln enthält). Weiter ist $k \equiv 1 \bmod 2$, da sonst $\sqrt{1 \pm i} \in L$ folgte. Indem wir $a+b\sqrt{m}$ notfalls mit einer geeigneten Potenz von u multiplizieren, dürfen wir k=1 annehmen.
Nun ist $\pi = a+b\sqrt{m} \equiv a-b\sqrt{m} = \pi' \bmod 2$, folglich $\zeta u = \pi^2/(1+i) \equiv \pi\pi'/(1+i) \equiv (1 \pm i)/(1+i) \equiv 1 \bmod (1+i)$, und da ζ eine 4. Einheitswurzel ist, gilt auch $\zeta \equiv 1 \bmod (1+i)$.

Bew. von (7.3).: Wir zeigen $M(L,I) \geq 5/4$ für das Ideal $I = (1+i)$; wegen $\Phi_L(I) = 2$ gibt es zwei prime Restklassen mod I. Dabei enthält die von 1 mod I verschiedene Restklasse keine Einheiten wegen (7.2); weiter enthält sie keine Elemente der Norm 3 (weil (3) in K prim ist). Die Behauptung folgt.

Wir geben noch eine kurze Tabelle einiger euklidischer Minima:

	disc K	M(K)	C_1	
i	144	1/2	sh. § 6, D(-1,2)	
1+i	512	1/2		
2+i	1280	5/4		$M_2 \leq 0.999$
3i	2304	5/2		
3+i	2560	5/4		$M_2 \leq 0.999$
1+3i	2560	5/4		$M_2 \leq 0.999$

Der Fall $L = K(\sqrt{p})$, $p \equiv \pm 1+2i \bmod 4$, ist schon etwas schwieriger; hier gilt aber

(7.5) Sei $L = K(\sqrt{p})$, $p \equiv \pm 1+2i \bmod 4$ prim; gibt es dann $s,t \in R$ mit $s \equiv t \equiv 1 \bmod 2$, $(s/p) = (t/p) = -1$, $(s,t) = 1$ und $|st| \leq k \cdot |p|$ für $k = \sqrt{2}/(1+\sqrt{2})$, dann ist L nicht normeuklidisch.
Hierbei ist $|\ |$ der gewöhnliche Betrag auf $\mathbb{C}$.

Bew.: Wir benutzen (1.4) Mit $B = (1+i)p$, $e=st$ und $k=1$; zu zeigen ist, daß es in R kein $r \equiv e \bmod (1+i)p$ gibt mit $N(r) < 2P$ und $r = N_{L/K}(\alpha)$ für ein $\alpha \in S$ (hier ist $P = N(p) = |p|^2$). Nun gilt $N(r) < 2P$, also $|r| < \sqrt{2}|p|$. Wir setzen $r = st + l(1+i)p$ für ein $l \in R$ und finden wegen $|st| \leq k|p|$ und $|r| < \sqrt{2}|p|$:

$$|l| \cdot \sqrt{2}|p| = |r-st| \leq |r| + |st| < (\sqrt{2}+k)|p| = 2|p|.$$

Also ist $|l| < \sqrt{2}$ und damit $l \in \{0, \pm 1, \pm i\}$. Wäre $l \equiv 1 \bmod (1+i)$, so folgte $r \equiv i \bmod 2$; ein solches r kann aber keine Norm aus S sein wegen

(7.6) Sei $L = K(\sqrt{m})$, $m \equiv \pm 1+2i \bmod 4$ und $\alpha \in S$. Dann ist $N_{L/K}(\alpha) \not\equiv i \bmod 2$.

Also ist l=0; dann ist r=st aber keine Norm aus S wegen (s,t)=1 und (s/p) = (t/p) = -1 (dies folgt wie im reellquadratischen Fall.

Wir müssen noch (7.6) beweisen: sei dazu $\alpha = (a+b\sqrt{m})/(1+i)$, $a \equiv b \bmod (1+i)$, und $N_{L/K}(\alpha) = c+di =: \beta$. Dann ist $a^2-mb^2 = 2i\beta$, und indem man diese Gleichung mod m und mod β betrachtet, folgt $[\frac{\beta}{m}] = [\frac{m}{\beta}] = +1$. Wäre nun $\beta \equiv \pm i \bmod 2$, so folgte aus dem QRG in R

$$[\tfrac{\beta}{m}] = [\tfrac{i}{m}][\tfrac{i\beta}{m}] = [\tfrac{i}{m}]\,[\tfrac{m}{i\beta}] = [\tfrac{i}{m}][\tfrac{m}{\beta}],$$

was aber wegen $[\frac{i}{m}] = -1$ im Widerspruch zu obigen Beobachtungen steht.

(7.7) Sei $L = K(\sqrt{p})$, $p \equiv \pm 1+2i \bmod 4$; dann ist L genau dann normeuklidisch, wenn $p \in \{1+2i,\ 3+2i,\ 5+2i,\ 1+6i,\ 7+2i\}$ ist.

Bew.: Daß L für p = 1+2i und p = 3+2i normeuklidisch ist, hat schon Lakein gezeigt. Ist L normeuklidisch, so hat van der Linden (1985, S. 163) gezeigt, daß disc L < 16·899.225 ist. Da in unserem Fall disc L = 64·N(p) ist, dürfen wir N(p) < 224.805 annehmen. Für diese p findet man mit einem Computer eine Darstellung wie in (7.4), es sei denn, es ist
$N(p) \in \{5, 13, 29, 37, 53, 61, 101, 157, 181, 229, 349, 541\}$.
Beispielsweise ist

P	p	s	t	P	p	s	t
109	3+10i	1-2i	1+2i	293	17+2i	1-2i	3
149	7+10i	1-2i	1+2i	317	11+14i	1-2i	3
173	13+2i	1+2i	3	373	7+18i	1+2i	3-2i
197	1+14i	1-2i	3	389	17+10i	1-2i	1+2i
269	13+10i	1-2i	1+2i	397	19+6i	1-2i	3-2i
277	9+14i	1+2i	1+4i	421	15+14i	1-2i	1+2i

Die $p \geq 101$ werden wir nun direkt mit (1.4) ausschließen:

P	p	e	B
61	5+6i	5	(1+i)p
101	1+10i	4-i	(p)
157	11+6i	-4+5i	(p)
181	9+10i	-4+5i	(p)
229	15+2i	4+i	(p)
349	5+18i	7i	(p)
541	21+10i	-5+14i	(1+i)p

Die für (7.7) nötige Rechenzeit läßt sich etwas verkürzen, wenn man das folgende Korollar von (7.5) benutzt:

(7.8) Sei $p \equiv \pm 1+2i \bmod 4$ prim, $N(p) \geq 109$, und $a \equiv \pm 2$, $b \equiv 0 \bmod 5$ oder $a \equiv 0$, $b \equiv \pm 1 \bmod 5$. Dann ist $L = K(\sqrt{p})$ nicht normeuklidisch.

Bew.: (7.5) mit $s = 1-2i$, $t = 1+2i$.

Auch hier geben wir einige euklidische Minima an:

m	disc K	M(K)	C_1
$1+2i$	320	1/2	
$3+2i$	832	1/2	
$5+2i$	1856		
$1+6i$	2368		
$3+6i$	2880		
$7+2i$	3392	$\geq 50/53$	

Der nächstschwierigere Fall ist nun $m \equiv 5 \bmod (1+i)^5$; hier gilt

(7.8) Sei $m \equiv 5 \bmod (1+i)^5$, $m \neq \pm 3$, und u die FE von L. Hat dann die Form $u = (x+y\sqrt{m})/(1+i)$ mit $x \equiv y \equiv 1 \bmod (1+i)$, dann ist L nicht normeuklidisch.

Bew.: Wir zeigen, daß das Ideal $(1+i)$ nicht euklidisch ist. Wegen $\Phi_L(1+i) = 3$, $\|(1+i)\| = 4$ und weil L keine Ideale der Norm 2 oder 3 enthält, genügt es zu zeigen, daß $u \equiv 1 \bmod (1+i)$ gilt. Dies folgt aber sofort aus $u-1 = (x-1 + (y-1)\sqrt{m})/(1+i)$, weil $(x-1 + (y-1)\sqrt{m})/2$ ganz ist.

Mit diesem Kriterium lassen sich jedoch nur wenige m ausschließen; immerhin gilt

(7.9) Sei $m \equiv \pm 3 \bmod (1+i)^5$ und $m = x^2 \pm 2$ für ein $x \in R$. Dann ist $(2+i+\sqrt{m})/(1-i) = ((1+\sqrt{m})/2)^3$ für $m = 1+4i$, während für alle andern m $u = (x+\sqrt{m})/(1+i)$ die FE ist.

Damit folgt z.B., daß L für die folgenden Werte von m nicht normeuklidisch sein kann:

$m = -11 = (3i)^2 - 2$ (sh. auch § 6)
$m = 7 + 12i = (3+2i)^2 + 2$, $P = 193$
$m = 13 + 8i = (4+i)^2 - 2$, $P = 233$
$m = 5 + 24i = (4+3i)^2 - 2$, $P = 601$
$m = 23 + 20i = (5+2i)^2 + 2$, $P = 929$.

Ein etwas nützlicheres Kriterium ist

(7.10) Sei $m \equiv \pm 3 \bmod (1+i)^5$, $s \equiv t \equiv 1 \bmod 2$, $(s,t) = 1$, $[s/m]=[t/m]=-1$ und $|st| \leq (\sqrt{2}-1)|m|$, $|st+m| \geq |m|$. Ist dann $|st-m| \geq |m|$ oder $st-m$ keine Norm aus S, dann ist $L = K(\sqrt{m})$ nicht normeuklidisch.

Bew.: Wir verwenden (1.4) mit $e=s\cdot t$ und beachten, daß aus $r=e+lm$, $l \in R$, $|lm| = |r-e| \leq |r|+|e| < |m| + (\sqrt{2}-1)|m| = \sqrt{2}|m|$, also $|l| < \sqrt{2}$ und damit $l \in \{0, \pm i, \pm 1\}$ folgt. Im Falle $l=0$ ist $r=e$ keine Norm; wäre $l=\pm i$, so folgte $r = e+lm \equiv 1+i \bmod 2$, und da $(1+i)$ in L/K träge ist, kann r dann keine Norm aus S sein. Damit bleiben nur noch die Möglichkeiten $l=1$, und die Voraussetzungen garantieren, daß dann $|r| \geq |m|$ oder r keine Norm aus S ist.