Binary quadratic forms over $\mathbb{Z}$ and quadratic fields

Basic question: find all solutions $(x,y)\in\mathbb{Z}^2$ of $\boxed{f(x,y)=ax^2+bxy+cy^2=m}$

$(a,b,c\in\mathbb{Z}, m\in\mathbb{Z}\setminus\{0\})$. The **discriminant** of f: $\Delta=\Delta(f)=b^2-4ac$ $(\equiv 0,1 \pmod 4)$.

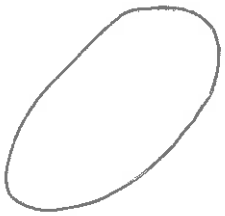
Easy case: $\sqrt{\Delta}\in\mathbb{Z} \Rightarrow f=\underbrace{(\alpha_1x+\beta_1y)}_{m_1}\underbrace{(\alpha_2x+\beta_2y)}_{m_2}$ is reducible over $\mathbb{Z}$ $(\alpha_i,\beta_i\in\mathbb{Z})$

$m_i\in\mathbb{Z}$, $m_1m_2=m$

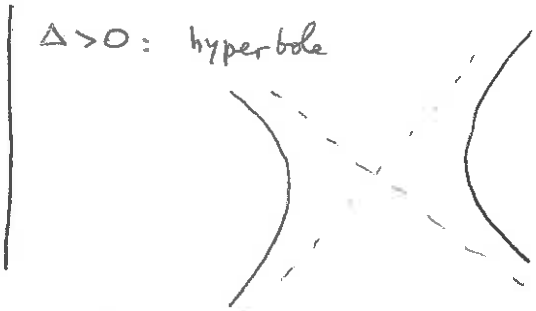
Interesting case: $\sqrt{\Delta}\notin\mathbb{Z}$ $(\Longleftrightarrow \sqrt{\Delta}\notin\mathbb{Q} \Longleftrightarrow f$ irreducible over $\mathbb{Q})$

Solutions in $\mathbb{R}^2$:

$\Delta<0$: ellipse



$\Delta>0$: hyperbole



Fact: $|\{\text{solutions in } \mathbb{Z}^2\}| = \begin{cases} \text{finite}, & \text{if } \Delta<0 \\ 0 \text{ or } \infty, & \text{if } \Delta>0 \end{cases}$ (proof: later)

Ex: $f(x,y)=2x^2-5y^2=\pm 3 \Longleftrightarrow 4x^2-10y^2=\underbrace{(2x+\sqrt{10}\,y)}_{\alpha}(2x-\sqrt{10}\,y)=\pm 6$ $(*)$

field $K=\mathbb{Q}(\sqrt{10})=\{u+v\sqrt{10} \mid u,v\in\mathbb{Q}\}$

$\cup$

ring $\mathbb{Z}[\sqrt{10}]=\{\text{---}''\text{---} \mid u,v\in\mathbb{Z}\}$

involution $\alpha=u+v\sqrt{10} \longmapsto \alpha'=u-v\sqrt{10}$

norm $N(\alpha)=\alpha\alpha'=u^2-10v^2$

$1,\sqrt{10}$ linearly independent over $\mathbb{Q}$

$\Downarrow$

$(\alpha\pm\beta)'=\alpha'\pm\beta'$, $(\alpha\beta)'=\alpha'\beta'$

$N(\alpha\beta)=N(\alpha)N(\beta)$

$(*) \Longleftrightarrow N(\alpha)=\pm 6$, $\alpha\in 2\mathbb{Z}+\sqrt{10}\,\mathbb{Z}\subset K$ $(*')$

Fact: $\left\{\begin{matrix}\text{Solutions}\\ \text{of } (*')\end{matrix}\right\} = \{\alpha=\underbrace{\pm}_{N=1}\underbrace{(2\pm\sqrt{10})}_{N=-6}\underbrace{(3+\sqrt{10})^n}_{N=(-1)^n} \mid n\in\mathbb{Z}\}$ (all 4 combinations of signs)

$N=6(-1)^{n+1}$

$\Updownarrow$

$\left\{\begin{matrix}\text{solutions}\\ \text{of } (*)\end{matrix}\right\} = \{(\pm x_n,\pm y_n) \mid 2x_n+\sqrt{10}\,y_n=(2+\sqrt{10})(3+\sqrt{10})^n,\ n\in\mathbb{Z}\}$ (—— " ——)

$$\begin{pmatrix}x_{n+1}\\ y_{n+1}\end{pmatrix}=\begin{pmatrix}3 & 5\\ 2 & 3\end{pmatrix}\begin{pmatrix}x_n\\ y_n\end{pmatrix}$$

n	-3	-2	-1	0	1	2	3
x_n	68	-11	2	1	8	49	302
y_n	-43	7	-1	1	5	31	191

Quadratic rings and fields

If $f(x,y) = ax^2 + bxy + cy^2 \Rightarrow$ $af(x,y) = \left(ax + \frac{b+\sqrt{\Delta}}{2}y\right)\left(ax + \frac{b-\sqrt{\Delta}}{2}y\right)$

$\Delta = b^2 - 4ac \equiv b \pmod 2$ $\quad cf(x,y) = \left(\frac{b+\sqrt{\Delta}}{2}x + cy\right)\left(\frac{b-\sqrt{\Delta}}{2}x + cy\right)$

Def. (1) $\Delta \in \mathbb{Z}$ is a **discriminant** if $\Delta \equiv 0, 1 \pmod 4$ $\left(\Leftrightarrow \exists a, b, c \in \mathbb{Z} \ \Delta = b^2 - 4ac\right)$

(Δ' discriminant, $n \in \mathbb{Z} \Rightarrow \Delta' n^2$ discriminant)

(2) A discriminant $\Delta \in \mathbb{Z}$ is **fundamental** if $\Delta = \Delta' n^2$, Δ' discriminant, $n > 1$

$\Updownarrow$

$$\Delta = \begin{cases} d & d \equiv 1 \pmod 4 \\ 4d & d \equiv 2, 3 \pmod 4 \end{cases}, \quad d \in \mathbb{Z} \setminus \{0\} \text{ square-free}$$

From now on: $\Delta \in \mathbb{Z}$ discriminant such that $\sqrt{\Delta} \notin \mathbb{Z}$ $\left(\Leftrightarrow \sqrt{\Delta} \notin \mathbb{Q}\right)$

Quadratic field $K = \mathbb{Q}(\sqrt{\Delta}) = \{u + v\sqrt{\Delta} \mid u, v \in \mathbb{Q}\}$ (real if $\Delta > 0$, imaginary if $\Delta < 0$)

$\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{\Delta n^2})$ for any $n \in \mathbb{Z} \setminus \{0\}$

Involution $\alpha = u + v\sqrt{\Delta} \longmapsto \alpha' = u - v\sqrt{\Delta}$, $(\alpha \pm \beta)' = \alpha' \pm \beta'$, $(\alpha\beta)' = \alpha'\beta'$, $\alpha' = \alpha \Leftrightarrow \alpha \in \mathbb{Q}$

Trace $Tr(\alpha) = Tr_{K/\mathbb{Q}}(\alpha) = \alpha + \alpha' = 2u$ (since $1, \sqrt{\Delta}$ are linearly independent over $\mathbb{Q}$)

Norm $N(\alpha) = N_{K/\mathbb{Q}}(\alpha) = \alpha\alpha' = u^2 - \Delta v^2$

Quadratic ring of discriminant Δ:

$$\mathcal{O}_\Delta = \mathbb{Z}\left[\frac{\Delta + \sqrt{\Delta}}{2}\right] = \begin{cases} \mathbb{Z}[\sqrt{\Delta/4}] = \{u + v\sqrt{\Delta/4} \mid u, v \in \mathbb{Z}\} & \text{if } \Delta \equiv 0 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{\Delta}}{2}\right] = \left\{u + v\frac{1+\sqrt{\Delta}}{2} \mid \text{—}\,''\,\text{—}\right\} & \text{if } \Delta \equiv 1 \pmod 4 \end{cases} \subset K$$

Ex: $\mathcal{O}_{-4} = \mathbb{Z}[i] \supset \mathbb{Z}[2i] = \mathcal{O}_{-16}$, $\mathcal{O}_{-3} = \mathbb{Z}[\zeta_3] \supset \mathcal{O}_{-12} = \mathbb{Z}[i\sqrt{3}]$; $\mathcal{O}_\Delta \supset \mathcal{O}_{\Delta n^2}$ $(n \geq 1)$

Why is K a field? Let $\alpha = u + v\sqrt{\Delta} \in K$.

$\alpha \neq 0 \Leftrightarrow u \neq 0$ or $v \neq 0 \Leftrightarrow$ ($\sqrt{\Delta} \notin \mathbb{Q}$) $\underbrace{u^2 - \Delta v^2}_{\alpha\alpha' = N(\alpha)} \neq 0 \Rightarrow \beta = N(\alpha)^{-1}\alpha' \in K$ and $\alpha\beta = 1$.

Units of $\mathcal{O}_\Delta$: $\mathcal{O}_\Delta^* = \{\alpha \in \mathcal{O}_\Delta \mid \exists \beta \in \mathcal{O}_\Delta \ \alpha\beta = 1\} = \{\alpha \in \mathcal{O}_\Delta \mid N(\alpha) \in \mathbb{Z}^* = \{\pm 1\}\}$

(if $\alpha\beta = 1 \Rightarrow N(\alpha)N(\beta) = N(1) = 1 \Rightarrow N(\alpha) \in \mathbb{Z}^*$; if $\alpha\alpha' \in \mathbb{Z}^* \Rightarrow \beta = (\alpha\alpha')^{-1}\alpha' \in \mathcal{O}_\Delta$, $\alpha\beta = 1$)

Explicitly: $\Delta \equiv 0 \pmod 4 \Rightarrow \mathcal{O}_\Delta^* = \{\alpha = u + v\sqrt{\Delta/4} \mid u, v \in \mathbb{Z},\ u^2 - (\Delta/4)v^2 = \pm 1\}$

$\Delta \equiv 1 \pmod 4 \Rightarrow \mathcal{O}_\Delta^* = \left\{\alpha = u + v\frac{1+\sqrt{\Delta}}{2} \mid u, v \in \mathbb{Z},\ u^2 + uv + \frac{1-\Delta}{4}v^2 = \frac{(2u+v)^2 - \Delta v^2}{4} = \pm 1\right\}$

Def. The **principal quadratic form of discriminant Δ** is

$$\begin{cases} x^2 - (\Delta/4)y^2 & \text{if } \Delta \equiv 0 \pmod 4 \\ x^2 + xy + \frac{1-\Delta}{4}y^2 & \text{if } \Delta \equiv 1 \pmod 4 \end{cases}$$

Interlude: solutions in $\mathbb{Q}^2$

(Δ discriminant, $\sqrt{\Delta} \notin \mathbb{Z}$, $m \in \mathbb{Z}\setminus\{0\}$)

$$f(x,y) = ax^2+bxy+cy^2 = m \iff am = \underbrace{(ax+by/2)}_{X}^2 - \Delta \underbrace{(y/2)}_{Y}^2 = X^2 - \Delta Y^2 = N(\alpha) \qquad (*)$$

$$\alpha = X + Y\sqrt{\Delta}$$

We know: $\exists X,Y \in \mathbb{Q}^2 \quad X^2-\Delta Y^2 = am \iff \forall v \in Pv\{\infty\} \quad \exists X_v, Y_v \in \mathbb{Q}_v^2 \quad X_v^2 - \Delta Y_v^2 = am$

Legendre

$$\Updownarrow$$

$$\text{—"—} \qquad \underbrace{(\Delta, am)_v = 1}_{\text{automatic if } v=p,\ p\nmid 2|am\Delta|}$$

If these conditions are satisfied, then $\exists\, \alpha_0 = X_0 + Y_0\sqrt{\Delta} \in K$ such that $N(\alpha_0) = am$ and there are bijections

$$\{\alpha = X+Y\sqrt{\Delta} \in K \mid N(\alpha) = X^2-\Delta Y^2 = am\} \longleftrightarrow \{\beta \in K \mid N(\beta) = 1\} \overset{\text{Hilbert 90}}{=\!=} \underbrace{\{\beta = \tfrac{\gamma}{\gamma'} \mid \gamma \in K^*\}}_{\text{abelian group isomorphic to } K^*/\mathbb{Q}^*}$$

$$\alpha \longmapsto \beta = \alpha/\alpha_0$$

$$\alpha = \beta\alpha_0 \longmapsto \beta$$

Conclusion: if $(x_0,y_0) \in \mathbb{Q}^2$ is a rational solution of $(*)$, then

$$\{\text{solutions } (X,Y) \in \mathbb{Q}^2 \text{ of } (*)\} = \{(X,Y) \in \mathbb{Q}^2 \mid \exists\, u,v \in \mathbb{Q},\ u\neq 0 \text{ or } v \neq 0 \quad X+Y\sqrt{\Delta} = (X_0+Y_0\sqrt{\Delta})\,\tfrac{u+v\sqrt{\Delta}}{u-v\sqrt{\Delta}}\}$$

Imaginary quadratic fields ($\Delta < 0$)

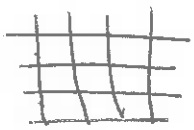
Geometric representation of $\mathcal{O}_\Delta$ and K:

Field embedding $K \hookrightarrow \mathbb{C}$, $\alpha' = \overline{\alpha}$, $N(\alpha) \geq 0$

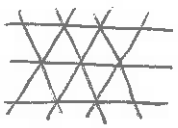
$$\alpha = u+v\sqrt{\Delta} \longmapsto u+vi\sqrt{|\Delta|}$$

$\mathcal{O}_\Delta \hookrightarrow \mathbb{C}$ lattice

Ex: $\Delta = -4$, $\mathcal{O}_{-4} = \mathbb{Z}[i]$ — square lattice



$\Delta = -3$, $\mathcal{O}_{-3} = \mathbb{Z}[\zeta_3]$



Units: $\mathcal{O}_\Delta^* = (\text{lattice } \mathcal{O}_\Delta) \cap (\text{unit circle})$

Prop. $\Delta < 0 \Rightarrow \mathcal{O}_\Delta^* = \begin{cases} \{\pm 1, \pm i\} = \mu_4 & \Delta = -4 \\ \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\} = \mu_6 & \Delta = -3 \\ \{\pm 1\} = \mu_2 & \Delta \neq -3, -4 \end{cases}$

Pf: If $\Delta = 4d$ ($d<0$): $\{u^2 + |d|v^2 = 1,\ u,v \in \mathbb{Z}\} \iff v=0,\ u=\pm 1$ OR $v=\pm 1,\ |d|=1,\ u=0$

If $\Delta \equiv 1 \pmod 4$: $\{(2u+v)^2 + |\Delta|v^2 = 4,\ u,v \in \mathbb{Z}\} \iff v=0,\ 2u+v=\pm 2 \iff v=0,\ u=\pm 1$ OR $|\Delta|=3,\ v=\pm 1,\ 2u+v=\pm 1$

Bounds for integral solutions of $ax^2+bxy+cy^2 = m$ ($\Delta<0 \Rightarrow ac \neq 0$)

$$(2ax+by)^2 + |\Delta|y^2 = 4am, \qquad |\Delta|x^2 + (bx+2cy)^2 = 4cm$$

$$\Rightarrow \underbrace{|y| \leq 2\left|\frac{am}{\Delta}\right|^{1/2}}, \qquad \underbrace{|x| \leq 2\left|\frac{cm}{\Delta}\right|^{1/2}}$$

Real quadratic fields ($\Delta > 0$, $\sqrt{\Delta} \notin \mathbb{Z}$)

Goal: thm. $\mathcal{O}_\Delta^* = \pm\varepsilon^{\mathbb{Z}} = \{\pm\varepsilon^n \mid n \in \mathbb{Z}\}$, $\varepsilon > 1$ the fundamental unit of $\mathcal{O}_\Delta$.

Ex: $\Delta = 40$, $\mathcal{O}_\Delta = \mathbb{Z}[\sqrt{10}]$, $\varepsilon = 3 + \sqrt{10}$.

Geometric representation of $\mathcal{O}_\Delta$ and K: $0 < \sqrt{\Delta} \in \mathbb{R}$

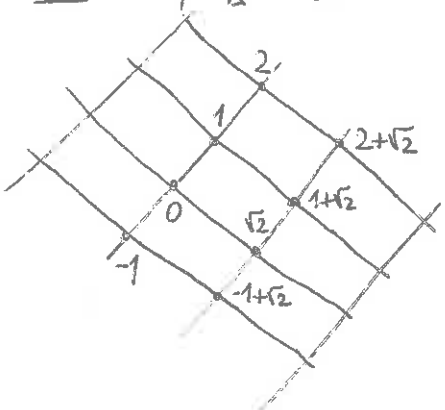
Two field embeddings

$$\mathbb{R} \xleftarrow{\sigma_1} K \xrightarrow{\sigma_2} \mathbb{R}$$
$$\alpha \longleftarrow \alpha \longmapsto \alpha'$$
$$u + v\sqrt{\Delta} \longleftarrow u + v\sqrt{\Delta} \longmapsto u - v\sqrt{\Delta}$$

$\sigma = (\sigma_1, \sigma_2) : K \hookrightarrow \mathbb{R} \times \mathbb{R}$, $\alpha \mapsto (\alpha, \alpha')$

$\sigma(\mathcal{O}_\Delta) \subset \mathbb{R}^2$ lattice, $\sigma_j(\mathcal{O}_\Delta) \subset \mathbb{R}$ dense

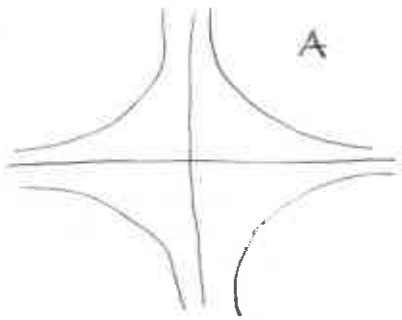
Ex: $\Delta = 8$, $\mathcal{O}_\Delta = \mathbb{Z}[\sqrt{2}]$



$$\begin{array}{ccccc} \mathcal{O}_\Delta^* & \subset & K^* & \xrightarrow{\sigma} & (\mathbb{R}^*)^2 \ni (x,y) \\ \downarrow N & & \downarrow N & & \downarrow N \quad \downarrow xy \\ \{\pm 1\} & \subset & \mathbb{Q}^* & \subset & \mathbb{R}^* \end{array}$$

Def: $A = \{(x,y) \in (\mathbb{R}^*)^2 \mid xy = \pm 1\}$ abelian group

Then: $\sigma(\mathcal{O}_\Delta^*) = \underbrace{\sigma(\mathcal{O}_\Delta)}_{\text{lattice}} \cap A$



Linearisation of A:

$$\lambda : A \xrightarrow{\sim} \{\pm 1\} \times \{\pm 1\} \times (\mathbb{R}, +)$$
$$(x,y) \longmapsto (xy,\ \operatorname{sgn}(x),\ \log|x|)$$

the logarithm map: (group morphism)

$$\mathcal{O}_\Delta^* \xrightarrow{\sigma} A \xrightarrow[\sim]{\lambda} \{\pm 1\}^2 \times \mathbb{R} \xrightarrow{pr_2} \mathbb{R}$$

$\ell' = pr_2 \circ \lambda$, $\ell = pr_2 \circ \lambda \circ \sigma$

$\ell(\alpha) = \log|\sigma_1(\alpha)| = \log|\alpha|$

Prop (1) $\operatorname{Ker}(\ell) = \{\pm 1\}$. (2) $\ell(\mathcal{O}_\Delta^*)$ is a discrete subgroup of $\mathbb{R}$.

Cor. Either $\ell(\mathcal{O}_\Delta^*) = 0$ $(\Rightarrow \mathcal{O}_\Delta^* = \{\pm 1\})$, or $\ell(\mathcal{O}_\Delta^*) = \mathbb{Z}\underbrace{\log|\varepsilon|}_{\neq 0}$ $(\Rightarrow \mathcal{O}_\Delta^* = \pm\varepsilon^{\mathbb{Z}})$.

Pf: (1) $\ell(\alpha) = 0 \Rightarrow |\alpha| = 1 \Rightarrow \alpha = \pm 1$ $(\alpha \in \mathbb{R}^*)$.

(2) Recall: (a) open subsets of any $X \subset \mathbb{R}^n$ are sets $X \cap U$, $U \subset \mathbb{R}^n$ open in $\mathbb{R}^n$;

(b) so $X \subset \mathbb{R}^n$ is a discrete subset of $\mathbb{R}^n \iff$ all subsets of X are open in X;

(c) for $X \subset \mathbb{R}^n$, $X' \subset \mathbb{R}^{n'}$, a homeomorphism $f : X \to X'$ is a bijection such that $U \subset X$ is open in $X \iff f(U)$ is open in X'.

The above group isomorphism $\lambda : A \xrightarrow{\sim} \{\pm 1\}^2 \times \mathbb{R}$ is a homeomorphism.

$\sigma(\mathcal{O}_\Delta) \subset \mathbb{R}^2$ is a discrete subset $\Rightarrow \sigma(\mathcal{O}_\Delta^*) \subset A$ is a discrete subgroup

$\Rightarrow \lambda(\sigma(\mathcal{O}_\Delta^*)) = \ell'(\mathcal{O}_\Delta^*) \subset \{\pm 1\}^2 \times \mathbb{R}$ is a discrete subgroup

$\Rightarrow$ $\underbrace{\ell(\mathcal{O}_\Delta^{*2})}_{\{0\} \text{ or } \mathbb{Z}\cdot\log(\varepsilon^2)} \subset \mathbb{R}$ ——— " ———

for some $\varepsilon \in \mathcal{O}_\Delta^* \setminus \{\pm 1\}$

$\Rightarrow \ell(\mathcal{O}_\Delta^*) = \{0\}$ or $\mathbb{Z}\cdot\log|\varepsilon|$.

Existence of units in $\mathcal{O}_\Delta^* - \{\pm 1\}$

To complete the proof of [Thm: $\mathcal{O}_\Delta^* = \pm\varepsilon^{\mathbb{Z}}$], we must show:

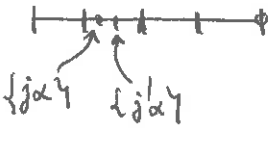
Prop. If $\Delta \in \mathbb{Z}$, $\Delta > 0$, $\sqrt{\Delta} \notin \mathbb{Z}$ $\Rightarrow \exists\, u, v \in \mathbb{Z}$, $v \neq 0$ $\quad u^2 - \Delta v^2 = \pm 1$.

this is done in two steps: diophantine approximation ($\left|\frac{u}{v}\right|$ is "close" to $\sqrt{\Delta}$) and descent.

Step 1. **Prop.** (Dirichlet) Let $\alpha \in \mathbb{R}$, $M \in \mathbb{Z}$, $M > 1$. Then $\exists\, p, q \in \mathbb{Z}$, $0 < q < M$, $|q\alpha - p| < \frac{1}{M}$ $(< \frac{1}{2})$.

Cor. $\forall \alpha \in \mathbb{R} - \mathbb{Q}$ $\exists$ infinitely many $\frac{p}{q} \in \mathbb{Q}$ $(p, q \in \mathbb{Z})$ such that $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

Pf of Prop. Subdivide $[0,1) = \bigsqcup_{i=0}^{M-1} \left[\frac{i}{M}, \frac{i+1}{M}\right)$ into M disjoint intervals of length $\frac{1}{M}$.



Among the $M+1$ fractional parts $\{j\alpha\} = j\alpha - \lfloor j\alpha \rfloor \in [0,1)$ $(0 \le j \le M)$ there must be two belonging to the same interval of subdivision:

$\exists\, 0 \le j < j' \le M$, $\exists\, 0 \le i < M$ $\quad \{j\alpha\}, \{j'\alpha\} \in \left[\frac{i}{M}, \frac{i+1}{M}\right)$

$$\Rightarrow \frac{1}{M} > |\{j'\alpha\} - \{j\alpha\}| = |\underbrace{(j'-j)}_{q}\alpha - (\lfloor j'\alpha \rfloor - \lfloor j\alpha \rfloor)|$$
$$\underbrace{\qquad\qquad}_{p}$$

Exercise. (1) Let $\alpha_1, \dots, \alpha_n \in \mathbb{R}$, $M \in \mathbb{Z}$, $M > 1$. Then $\exists\, p_1, \dots, p_n, q \in \mathbb{Z}$, $0 < q < M^n$ $\forall i = 1, \dots, n$ $|q\alpha_i - p_i| < \frac{1}{M}$

(2) —— " —— , $t \in \mathbb{R}$, $t > 1$. —— " —— , $0 < q < t$ — " —— $|q\alpha_i - p_i| \le \frac{1}{t^{1/n}}$.

[Hint: apply Minkowski's thm to $\{(x_0, \dots, x_n) \in \mathbb{R}^{n+1} \mid |x_0| < c,\ |x_0\alpha_i - x_i| \le c'\ \forall i \neq 0\}$]

Cor. $\exists$ infinitely many $(p_n, q_n) \in \mathbb{Z}^2$ such that $\left|\frac{p_n}{q_n} - \sqrt{\Delta}\right| < \frac{1}{q_n^2} \Rightarrow \left|\frac{p_n}{q_n} + \sqrt{\Delta}\right| < \frac{1}{q_n^2} + 2\sqrt{\Delta} \le (2\sqrt{\Delta} + 1)$

$$\Rightarrow |p_n^2 - \Delta q_n^2| = q_n^2 \left|\frac{p_n}{q_n} - \sqrt{\Delta}\right| \cdot \left|\frac{p_n}{q_n} + \sqrt{\Delta}\right| < (2\sqrt{\Delta} + 1) =: C.$$

Step 2 (descent) So $\exists$ infinitely many $\alpha_n = p_n + q_n\sqrt{\Delta} \in \mathbb{Z}[\sqrt{\Delta}] \subset \mathcal{O}_\Delta$ such that $|N(\alpha_n)| < C$.

After replacing $\{\alpha_n\}$ by a subsequence, we can first assume that

(a) $\forall n$ $\quad N(\alpha_n) = m$ $\quad (m \in \mathbb{Z}$ fixed, $|m| < C)$ $\quad (m \neq 0$, since $N(\alpha) = 0 \Leftrightarrow \alpha = 0)$

and then

(b) $\forall n$ $\quad p_n \equiv p_{n+1} \pmod m$, $\quad q_n \equiv q_{n+1} \pmod m$ $\quad (\Leftrightarrow \alpha_n \equiv \alpha_{n+1} \pmod{m\mathbb{Z}[\sqrt{\Delta}]})$

Then $\alpha_n' \alpha_{n+1} \equiv \alpha_n' \alpha_n = N(\alpha_n) = m \equiv 0 \pmod{m\mathbb{Z}[\sqrt{\Delta}]} \Rightarrow \alpha_n' \alpha_{n+1} = m\beta_n$,

$\beta_n \in \mathbb{Z}[\sqrt{\Delta}]$, $N(\beta_n) = \frac{N(\alpha_n')\, N(\alpha_{n+1})}{N(m)} = \frac{m \cdot m}{m^2} = 1 \Rightarrow \beta_n \in \mathbb{Z}[\sqrt{\Delta}]^*$.

β_n are distinct $\Rightarrow$ one among $\beta_1, \beta_2, \beta_3$ satisfies $\beta_n \neq \pm 1$.

So $\beta_n = u + v\sqrt{\Delta}$, $v \neq 0$, $u^2 - \Delta v^2 = \pm 1$.

Summary: we have proved: **Thm** $\forall$ discriminant $\Delta > 0$ such that $\sqrt{\Delta} \notin \mathbb{Z}$

$\exists!\, \varepsilon \in \mathcal{O}_\Delta^*$ such that $\mathcal{O}_\Delta^* = \underbrace{\pm\varepsilon^{\mathbb{Z}}}_{\{\pm\varepsilon^n \mid n \in \mathbb{Z}\}}$ and $\varepsilon > 1$ (ε = the fundamental unit of $\mathcal{O}_\Delta$).

Note. $\forall n \ge 1$ $\exists\, a(n) \ge 1$ such that $\varepsilon^{a(n)}$ = the fundamental unit of $\mathcal{O}_{\Delta n^2}$.

Ex: $\varepsilon = 1 + \sqrt{2}$ = fundamental unit of $\mathbb{Z}[\sqrt{2}] = \mathcal{O}_8$, $\varepsilon^2 = 3 + 2\sqrt{2}$ fund. unit of $\mathbb{Z}[2\sqrt{2}] = \mathcal{O}_{32}$.

Frequently asked questions about $\mathcal{O}_\Delta^*$

(1) How big is the fundamental unit $\varepsilon \in \mathcal{O}_\Delta^*$?

Easy to show: $\exists$ explicit constant $C>0$ such that $\log(\varepsilon) < C\cdot\Delta$

More difficult (Siegel): $\forall \delta>0$ $\exists$ non-explicit constant $C(\delta)>0$ such that $\log(\varepsilon) < C(\delta)\Delta^{\frac{1}{2}+\delta}$

Ex: $\mathbb{Z}[\sqrt{31}]^*$: $\varepsilon = 1520 + 273\sqrt{31}$; $\mathbb{Z}[\sqrt{46}]^*$: $\varepsilon = 24\,335 + 3588\sqrt{46}$

$\mathbb{Z}[\sqrt{94}]^*$: $\varepsilon = 2\,143\,295 + 221\,064\sqrt{94}$; $\mathbb{Z}[\sqrt{991}]^*$: $\varepsilon =$ truly monstrous

---

(2) Is $N(\varepsilon) = +1$ or -1 ? There is no explicit criterion in terms of Δ. However:

Prop. If $p \equiv 1 \pmod 4$ is a prime $\Rightarrow \exists\, \eta \in \mathbb{Z}[\sqrt{p}]^*$ $N(\eta) = -1 \Rightarrow \exists\, \eta' \in \mathbb{Z}\left[\frac{1+\sqrt{p}}{2}\right]^*$ $N(\eta') = -1$.

Pf. Let $\varepsilon = x + y\sqrt{p}$ $(x>1, y\geq 1)$ be the fundamental unit of $\mathbb{Z}[\sqrt{p}] = \mathcal{O}_{4p}$; $N(\varepsilon) = \pm 1$.

If $N(\varepsilon) = x^2 - py^2 = 1 \overset{(\mathrm{mod}\,4)}{\Longrightarrow} 2 \mid y$, $2 \nmid x$, $\frac{x+1}{2}\cdot\frac{x-1}{2} = p(y/2)^2$. As $\frac{x+1}{2} = 1 + \frac{x-1}{2}$, $\gcd\left(\frac{x+1}{2}, \frac{x-1}{2}\right) = 1$

$\Rightarrow \exists u, v \in \mathbb{Z}_{>0}$ $\left(\frac{x+1}{2} = u^2,\ \frac{x-1}{2} = pv^2\right)$ or $\left(\frac{x-1}{2} = u^2,\ \frac{x+1}{2} = pv^2\right) \Rightarrow \eta = u + v\sqrt{p}$, $N(\eta) = \pm 1$

$\Rightarrow \eta \in \mathbb{Z}[\sqrt{p}]^*$, $1 < \eta < \varepsilon$ — contradiction. Therefore $N(\varepsilon) = -1$.

Note: $d \equiv 3 \pmod 4 \Rightarrow x^2 - dy^2 = -1$ has no solution $\pmod 4 \Rightarrow$ no solution in $\mathbb{Z}^2$.

(3) How can one find ε explicitly? Using the best rational approximations to $\sqrt{\Delta/4}$ resp. $\frac{1+\sqrt{\Delta}}{2}$, given by continued fractions.

Ex: (a) $\mathcal{O}_{28}^* = \mathbb{Z}[\sqrt{7}]^*$: $\textcircled{2} < \sqrt{7} < 3$ $\alpha_0 = \sqrt{7} = 2 + \frac{1}{\alpha_1}$; $\alpha_1 = \frac{1}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{3}$, $\textcircled{1} < \alpha_1 < 2$,

$\alpha_1 = 1 + \frac{1}{\alpha_2}$; $\alpha_2 = \frac{3}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{2}$, $\textcircled{1} < \alpha_2 < 2$, $\alpha_2 = 1 + \frac{1}{\alpha_3}$; $\alpha_3 = \frac{2}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{3}$, $\textcircled{1} < \alpha_3 < 2$,

$\alpha_3 = 1 + \frac{1}{\alpha_4}$; $\alpha_4 = \frac{3}{\sqrt{7}-2} = \sqrt{7}+2 = \alpha_0 + 2$, $\textcircled{4} < \alpha_4 < 5$, $\alpha_4 = 4 + \frac{1}{\alpha_5}$; $\underline{\alpha_5 = \alpha_1}$

$$\sqrt{7} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cdots}}}}}}}} = [2,1,1,1,4,1,1,1,4,\ldots] = [2,\overline{1,1,1,4}]$$ ultimately periodic

$$[2,1,1,1] = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}} \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} \begin{matrix} 2 \\ \frac{3}{2} \end{matrix} \Bigg\} \frac{2}{3} = \frac{8}{3}$$

$\varepsilon = 8 + 3\sqrt{7}$, $N(\varepsilon) = 8^2 - 7\cdot 3^2 = 1$

(b) $\mathcal{O}_{13}^* = \mathbb{Z}\left[\frac{1+\sqrt{13}}{2}\right]^*$: $\alpha_0 = \frac{\sqrt{13}+1}{2}$, $\textcircled{2} < \alpha_0 < 3$; $\alpha_0 = 2 + \frac{1}{\alpha_1}$; $\alpha_1 = \frac{2}{\sqrt{13}-3} = \frac{\sqrt{13}+3}{2} = \alpha_0 + 1$,

$\textcircled{3} < \alpha_1 < 4$, $\alpha_1 = 3 + \frac{1}{\alpha_2}$; $\underline{\alpha_2 = \alpha_1}$ $\quad \frac{\sqrt{13}+1}{2} = 2 + \cfrac{1}{3 + \cfrac{1}{3 + \cfrac{1}{3 + \cdots}}} = [2,\overline{3}]$, $[2] = \frac{2}{1}$

$\varepsilon = 2 + 1\cdot\frac{-1+\sqrt{13}}{2} = \frac{3+\sqrt{13}}{2}$, $N(\varepsilon) = \frac{3^2 - 13\cdot 1^2}{4} = -1$

---

(4) What about $x^3 - 2y^3 = \pm 1$?

$$(x - y\sqrt[3]{2})(x - y\zeta_3\sqrt[3]{2})(x - y\zeta_3^2\sqrt[3]{2}) = \alpha\alpha'\alpha''$$

problem: $(x + y\sqrt[3]{2})(x' + y'\sqrt[3]{2}) = xx' + (xy' + yx')\sqrt[3]{2} + yy'\sqrt[3]{4}$ also involves $\sqrt[3]{4}$!!

One must consider $\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} = \alpha \mid a,b,c \in \mathbb{Z}\}$; then

$\mathbb{Z}[\sqrt[3]{2}]^* = \{\alpha \in \mathbb{Z}[\sqrt[3]{2}] \mid N(\alpha) = \alpha\alpha'\alpha'' = \pm 1\} = \{\pm\varepsilon^n \mid n \in \mathbb{Z}\}$ $\quad \varepsilon = 1 + \sqrt[3]{2}$

$\alpha' = a + b\zeta_3\sqrt[3]{2} + c\zeta_3^2\sqrt[3]{4}$ $\quad N(\alpha) = a^3 + 2b^3 + 4c^3 - 6abc$

$\alpha'' = a + b\zeta_3^2\sqrt[3]{2} + c\zeta_3\sqrt[3]{4}$

Bounds on the size of the smallest solutions

$\Delta(f) = \Delta > 0$, $\sqrt{\Delta} \notin \mathbb{Z}$, $m \in \mathbb{Z} \setminus \{0\}$

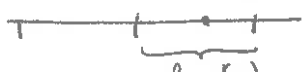
$f(x,y) = ax^2 + bxy + cy^2 = \pm m \iff \pm am = \underbrace{\left(ax + \frac{b+\sqrt{\Delta}}{2} y\right)}_{\alpha} \underbrace{\left(ax + \frac{b-\sqrt{\Delta}}{2} y\right)}_{\alpha'} = N(\alpha)$

$(x,y \in \mathbb{Z})$

(*) $\alpha \in I$, $|N(\alpha)| = |am|$ $\iff$ $\alpha \in I = \mathbb{Z}a + \mathbb{Z}\frac{b+\sqrt{\Delta}}{2} \subset \mathcal{O}_\Delta$ subgroup (of finite index) such that $\forall \beta \in \mathcal{O}_\Delta$ $\beta I \subset I$ (I = an ideal of $\mathcal{O}_\Delta$)

Prop. Let $\eta \in \mathcal{O}_\Delta^*$, $\eta > 1$. $\forall$ solution α of (*) $\exists k \in \mathbb{Z}$ such that $\underbrace{\beta = \eta^{-k}\alpha}_{u+v\sqrt{\Delta}}$ is also a solution of (*) and $|\beta|, |\beta'| \le |am\eta|^{1/2}$ ($\Rightarrow |u|, |v\sqrt{\Delta}| \le |am\eta|^{1/2}$), $u, v \in \mathbb{Z}$ or $\frac{1}{2}+\mathbb{Z}$

Pf: $|\eta\eta'| = 1$. $\exists k \in \mathbb{Z}$ $\left| \log \frac{|\alpha|}{|am|^{1/2}} - k \log(\eta) \right| \le \frac{1}{2}\log(\eta)$



$\Rightarrow \beta = \eta^{-k}\alpha \in I$, $\eta^{-1/2} \le \frac{|\beta|}{|am|^{1/2}} \le \eta^{1/2}$, $|\beta\beta'| = |am| \Rightarrow \frac{|\beta'|}{|am|^{1/2}} \le \eta^{1/2}$.

Example: $x^2 - 79y^2 = \pm m$ $\quad m \in \mathbb{Z} \setminus \{0\}$

$\eta = 80 + 9\sqrt{79}$, $N(\eta) = 1$ (in fact, $\eta = \varepsilon$ the fundamental unit of $\mathbb{Z}[\sqrt{79}]$)

Elementary observation: $x^2, y^2 \equiv 0, 1, 4 \pmod 8 \Rightarrow x^2 - 79y^2 \equiv x^2 + y^2 \not\equiv -1, -2, 3 \pmod 8$

(so no solution in $\mathbb{Z}^2$ if $m \equiv -1, -2, 3 \pmod 8$)

Scientific observation: $\exists$ solution $(x,y) \in \mathbb{Q}^2 \iff \forall$ prime p $(79, m)_p = 1$

$-79 \in 1 + 8\mathbb{Z}_2 = \mathbb{Z}_2^*$; if $m = 2^i m'$, $2 \nmid m' \Rightarrow (79, m)_2 = \underbrace{(-1, 2)_2^i}_{1} (-1, m')_2 = (-1)^{\frac{m'-1}{2}}$

(so if $m \equiv -1, -2, 3 \pmod 8 \Rightarrow (79, m)_2 = -1 \Rightarrow$ no solution in $\mathbb{Q}^2$).

Prop. above says: if $\alpha = x + y\sqrt{79}$, $x, y \in \mathbb{Z}$, $N(\alpha) = x^2 - 79y^2 = m$, then $\exists k \in \mathbb{Z}$ such that $\beta = \eta^{-k}\alpha = u + v\sqrt{79}$ satisfies $N(\beta) = u^2 - 79v^2 = m\,N(\eta)^{-k} = m$ and

$|u|, |v|\sqrt{79} \le |m\eta|^{1/2} < 4|10m|^{1/2}$ (since $\eta < 160$).

$m = 2$ ($\Rightarrow 2 \nmid uv$): $|v|\sqrt{79} < 4\sqrt{20} < 18 \Rightarrow |v| \le 2$ $\lightning$ $\Rightarrow |v| = 1$ $\qquad 79 \cdot 1^2 + 2 = 81 = 9^2$

$\beta = \pm(9 \pm \sqrt{79})$ $\qquad$ ($2 \nmid v$)

$\alpha = \pm(9 \pm \sqrt{79})(80 + 9\sqrt{79})^n$, $n \in \mathbb{Z}$

$m = -3$: $|u|, |v|\sqrt{79} < 4\sqrt{30} < 22 \Rightarrow |v| \le 2$

v	0	1	2	
$-3 + 79v^2$	-3	76	313	$\neq u^2$

no solution $(x,y) \in \mathbb{Z}^2$ of $x^2 - 79y^2 = -3$

Exercise: $x^2 - 79y^2 = -3$ has a solution in all $\mathbb{Z}_p$ (Hensel's lemma + ε).

($\iff x^2 - 79y^2 \equiv -3 \pmod n$ — " — $\forall n \ge 1$)

Note: $79 = 2^2 + 3 \cdot 5^2 \Rightarrow (2/5)^2 - 79(1/5)^2 = -3$

Conclusion: the Minkowski–Hasse theorem does NOT hold if we replace $\mathbb{Q}, \mathbb{Q}_p$ by $\mathbb{Z}, \mathbb{Z}_p$.

Rmk: $\Delta = 4 \cdot 79$ is the (second) smallest positive fundamental discriminant for which this phenomenon occurs.

Solutions of $ax^2+bxy+cy^2 = \pm m$ $(\Delta>0,\ \sqrt{\Delta}\notin\mathbb{Z})$ – summary

$$\Updownarrow$$

$$|N(\alpha)| = |am| \ , \quad \alpha \in I = \mathbb{Z}a + \mathbb{Z}\,\frac{b+\sqrt{\Delta}}{2} \qquad (*)$$

Assume $\eta \in O_\Delta^* = \langle \pm\eta \rangle$. Then:

$$\{\, \beta \in I \mid |N(\beta)| = |am| \ , \ |\beta|, |\beta'| \le |am\eta|^{1/2} \,\} = \{\beta_1, \dots, \beta_r\} \qquad (r \ge 0)$$

is finite (possibly empty) and

$$\{\text{solutions } \alpha \in I \text{ of } (*)\} = \{\beta_1\eta^n, \dots, \beta_r\eta^n \mid n \in \mathbb{Z}\}$$

Exercise: Find all solutions of

$$19x^2 + 22xy + 6y^2 = \pm 3, \pm 5 \qquad (x,y \in \mathbb{Z})$$

[Hint: determine first if there are solutions $x,y \in \mathbb{Q}$]