Representability of integers by $ax^2+bxy+cy^2$ – examples

Recall: $x^2-79y^2=-3$ has no solution in $\mathbb{Z}^2$, but it has solutions in $\mathbb{R}^2$ and all $\mathbb{Z}_p^2$ ($x^2-79y^2\equiv -3 \pmod n$ has a solution for all $n\geq 1$). Idem for $x^2-34y^2=-1$.

What is going on? Let us look at some examples with $\Delta<0$.

Notation: if $f=ax^2+bxy+cy^2$ is positive definite ($\Leftrightarrow \Delta=b^2-4ac<0<a,c$), let

$$S(f)=\{n\in\mathbb{Z}_{>0} \mid \exists\, x,y\in\mathbb{Z} \quad f(x,y)=n\} = \bigcup_{d\geq 1} d^2 S_{prim}(f)$$

$S_{prim}(f)=\{$ —— " —— , $\gcd(x,y)=1$, — " — $\}$

Multiplicativity: if $f(x,y)=(x+\alpha y)(x+\alpha' y)$ is the principal form ($\alpha=\left\{\frac{\sqrt{\Delta}/2}{\frac{1+\sqrt{\Delta}}{2}}\right\}$), then $N(\beta\gamma)=N(\beta)N(\gamma)$ implies that $[m,n\in S(f) \Rightarrow mn\in S(f)]$

Example 1: $\boxed{f=x^2+y^2}$ $(\Delta=-4)$

We have

(D) **Descent property**: if $n \mid N\in S_{prim}(f) \Rightarrow n\in S_{prim}(f)$ $(\Leftrightarrow \mathbb{Z}[i]$ is a UFD)

Pf: The proof we gave when $n=p$ is a prime works in general.

(R) **Reciprocity property**: an integer $n\geq 1$ divides some $N\in S_{prim}(f)$

$\Updownarrow$

$\exists\, x,y\in\mathbb{Z}$, $\gcd(x,y)=1$, $x^2+y^2\equiv 0 \pmod n$ $(\Rightarrow \gcd(x,n)=\gcd(y,n)=1$, $\exists\, t\in\mathbb{Z}$ $x\equiv ty \pmod n)$

$\exists\, t\in\mathbb{Z}$ $n=\prod p^{v_p(n)}$

$\Updownarrow$

$t^2+1\equiv 0 \pmod n$

$\Updownarrow$

$4\nmid n \wedge \forall\, p\mid n, p\neq 2 \quad \left(\frac{-1}{p}\right)=1 \Leftrightarrow 4\nmid n \wedge \forall p\mid n, p\neq 2 \quad p\equiv 1 \pmod 4$

Conclusion: $S_{prim}(x^2+y^2)=\left\{ n\geq 1 \mid n=2^b \prod_{p_i\equiv 1 \pmod 4} p_i^{a_i},\ b\leq 1\right\}$

$\mathbb{P}\cap S(x^2+y^2)=\{2\}\cup\{p\equiv 1 \pmod 4\}$

Exercise: (1) For $f=x^2+2y^2$ $(\Delta=-8)$. (D) holds ($\mathbb{Z}[i\sqrt{2}]$ is a UFD) and (R) says: n divides some $N\in S_{prim}(f) \Leftrightarrow \exists\, t\in\mathbb{Z}$ $t^2+2\equiv 0 \pmod n$

$\Leftrightarrow 4\nmid n$ $\forall\, p\nmid n, p\neq 2$ $\left(\frac{-2}{p}\right)=1$ $(\Leftrightarrow p\equiv 1,3 \pmod 8)$,

$$S_{prim}(x^2+2y^2)=\left\{ n\geq 1 \mid n=2^b \prod_{p_i\equiv 1,3 \pmod 8} p_i^{a_i},\ b\leq 1\right\}$$

(2) For $f=x^2+xy+y^2$ $(\Delta=-3)$ (D) holds ($\mathbb{Z}[\zeta_3]$ is a UFD) and (R) says: $n \mid$ some $N\in S_{prim}(f) \Leftrightarrow \exists\, t\in\mathbb{Z}$ $t^2+t+1\equiv 0 \pmod n$.

Find $S_{prim}(f)$.

(3) What happens for $f=x^2+3y^2$ $(\Delta=-12)$? $2\cdot 2=(1+i\sqrt{3})(1-i\sqrt{3})$

Example 2 : $\boxed{f = x^2+5y^2}$ $(\Delta = -20)$

$S_{prim}(f) = \{1, 5, 6, 9, 14, 21, 29, 30, 41, 45, 46, 49, 54, 61, 69, 70, 81, 86, 89, 94, \dots\}$

$P \cap S(f) = \{5, 29, 41, 61, 89, \dots\}$ $\quad m, n \in S(f) \Rightarrow mn \in S(f)$

Descent fails ! $\mathbb{Z}[i\sqrt{5}]$ does not have unique factorisation

$21 = 3\cdot 7 \in S_{prim}(f) \not\ni 3, 7 \qquad 3\cdot 7 = (4+i\sqrt{5})(4-i\sqrt{5})$

Observe : (1) $3\cdot 7 \in S_{prim}(f)$, $3, 7 \notin S_{prim}(f)$, but $2\cdot 3, 2\cdot 7 \in S_{prim}(f)$

(2) $2n \in \underset{prim}{S(f)} \iff 2n = u^2+5v^2 \iff u = 2x+y$, $v = y$ $(x, y \in \mathbb{Z})$, $\gcd(u, v) = 1$, $\gcd(2x, y) = 1$

$n = \dfrac{(2x+y)^2+5y^2}{2} = \underbrace{2x^2+2xy+3y^2}_{f'(x,y)}$ $\qquad \Delta(f') = \Delta(f) = -20$

(3) So we get another form f' with $\Delta(f') = -20$,

$S_{prim}(f') = \left(\frac{1}{2} S_{prim}(f) \cap \mathbb{Z}\right) \cup 2 S_{prim}(f) = \{2, 3, 7, 10, 15, 18, 23, 27, 35, 42, 43, 47, \dots\}$

$P \cap S(f') = \{2, 3, 7, 23, 43, 47, \dots\}$

It seems that : • $S(f) \cap P \overset{?}{=} \{5\} \cup \{p \equiv 1, 9 \pmod{20}\}$

• $S(f') \cap P \overset{?}{=} \{2\} \cup \{p \equiv 3, 7 \pmod{20}\} \overset{?}{=} \{2\} \cup \left(\frac{1}{2} S(f) \cap P\right)$

• $m \in S(f)$, $n' \in S(f') \overset{?}{\Rightarrow} mn' \in S(f')$

• $m', n' \in S(f') \overset{?}{\Rightarrow} m'n' \in S(f)$

Explanation : multiplicativity :

$$(x^2+5y^2)(2x'^2+2x'y'+3y'^2) = 2(xx'-yx'-3yy')^2 + 2(xx'-yx'-3yy')(xy'+2yx'+2yy') + 3(xy'+2yx'+2yy')^2$$

$$(2x^2+2xy+3y^2)(2x'^2+2x'y'+3y'^2) = (2xx'+xy'+yx'+3yy')^2 + 5(xy'-yx')^2 \quad \text{(Lagrange)}$$

Congruence conditions : Prop. If $p \mid (ax^2+bxy+cy^2)$, $\gcd(x, y) = 1$, p prime $\Rightarrow \exists t \in \mathbb{Z}$ $t^2 \equiv \Delta \pmod{p}$

Pf : $p \mid (2ax+by)^2 - \Delta y^2$ and $p \nmid x$ or $p \nmid y \Rightarrow \exists t \in \mathbb{Z}$ $t^2 \equiv \Delta \pmod{p}$.
$p \mid (2cy+bx)^2 - \Delta x^2$

$(\Rightarrow p \mid \Delta$ or $\left(\frac{\Delta}{p}\right) = 1$, if $p \neq 2)$

Our case : if $p \neq 2, 5$ prime, $p \mid n \in S_{prim}(f)$ or $p \mid n' \in S_{prim}(f') \Rightarrow \underline{\left(\frac{-20}{p}\right) = 1}$.

Reciprocity property : rewrite the condition $\left(\frac{-20}{p}\right) = \left(\frac{-4}{p}\right)\left(\frac{5}{p}\right) = 1$ $\qquad -20 = (-4)\cdot 5$ (discriminants)

$\chi_{-20}(p)$ $\quad \chi_{-4}(p)$ $\quad \chi_5(p)$

$\chi_{-4} : (\mathbb{Z}/4\mathbb{Z})^* \longrightarrow \{\pm 1\}$, $a \longmapsto (-1)^{\frac{a-1}{2}}$ $\qquad$ $\chi_5 : (\mathbb{Z}/5\mathbb{Z})^* \longrightarrow \{\pm 1\}$, $a \longmapsto \left(\frac{a}{5}\right)$

$\chi_{-4}(a) = \begin{cases} 1 & a \equiv 1 \ (4) \\ -1 & a \equiv -1 \ (4) \end{cases}$ $\qquad$ $\chi_{*5}(a) = \begin{cases} 1 & a \equiv \pm 1 \ (5) \\ -1 & a \equiv \pm 2 \ (5) \end{cases}$ $\qquad$ $\chi_{-20} = \chi_{-4}\chi_5 : (\mathbb{Z}/20\mathbb{Z})^* \longrightarrow \{\pm 1\}$

$$\chi_{-20}(a) = 1 \iff \begin{cases} \chi_{-4}(a) = \chi_5(a) = 1 \iff a \equiv 1, 9 \pmod{20} \\ \chi_{-4}(a) = \chi_5(a) = -1 \iff a \equiv 3, 7 \pmod{20} \end{cases}$$

So $\left(\frac{-20}{p}\right) = 1 \iff p \equiv 1, 3, 7, 9 \pmod{20}$.

It seems that: $p \equiv 1, 9 \pmod{20}$

$P \cap S(f) \stackrel{?}{=} \{5\} \cup \{p \mid \chi_{-4}(p) = \chi_5(p) = 1\}$

$P \cap S(f') \stackrel{?}{=} \{2\} \cup \{p \mid \chi_{-4}(p) = \chi_5(p) = -1\}$ $\quad p \equiv 3, 7 \pmod{20}$

$S_{prim}(f) \cap \{n \mid \gcd(n, 20) = 1\} = \{1, 9, 21, 29, 41, 49, 61, 69, 81, 89, \dots\}$

$\stackrel{?}{=} \{ \text{---} \,''\, \text{---}, \forall p \mid n \ \chi_{-20}(p) = 1, \ \chi_{-4}(n) = \chi_5(n) = 1\}$ $\quad n \equiv 1, 9 \pmod{20}$

$S_{prim}(f') \cap \{n \mid \gcd(n, 20) = 1\} = \{3, 7, 23, 27, 43, 47, \dots\}$

$\stackrel{?}{=} \{ \text{---} \,''\, \text{---}, \forall p \mid n \ \chi_{-20}(p) = 1, \ \chi_{-4}(n) = \chi_5(n) = -1\}$

$p \equiv 1, 3, 7, 9 \pmod{20}$ $\quad n \equiv 3, 7 \pmod{20}$

TRUE!

So we have two classes of forms with $\Delta = -20$,

$f = x^2 + 5y^2$ and $f' = 2x^2 + 2xy + 3y^2$.

Over $\mathbb{Q}$: $f = \langle 1, 5 \rangle$, $f' \sim \langle 2, 10 \rangle$

$(2, 10)_5 = (2, 5)_5 = \left(\frac{2}{5}\right) = -1 \neq 1 = (1, 5)_5 \Rightarrow$ f, f' are not equivalent over $\mathbb{Q}$

Representability of integers $n \geq 1$ by f resp. f' is given by appropriate congruence conditions on n and on all primes dividing n.

Ex: $\boxed{f_1 = x^2+14y^2}$, $\boxed{\Delta = -56}$

$S(f_1)_{prim} = \{15, 18, 23, 30, 39, 50, 57, 63, 65, 78, 81, 95, 105, 114, 127, 130, 135, 137, 142, \dots\}$

$S(f_1)_{prim} \cap \{n \mid \gcd(n,56)=1\} = \{15, 23, 39, 57, 65, 81, 95, 127, 135, 137, 151, 177, 183, \dots\}$

$S(f_1) \cap \mathbb{P} = \{23, 127, 137, 151, \dots\}$

Descent property does not hold: $3\cdot 5 \in S(f_1)_{prim} \not\ni 3, 5$

$\Updownarrow$

$\mathbb{Z}[i\sqrt{14}]$ is not a UFD: $3\cdot 5 = (1+i\sqrt{14})(1-i\sqrt{14})$

If $2n = x^2+14y^2 \Rightarrow n = 2(x/2)^2+7y^2$. Consider $\boxed{f_2 = 2x^2+7y^2}$, $\Delta(f_2) = -56$

$S(f_2)_{prim} = \{9, 15, 25, 30, 39, 46, 57, 65, 71, 78, 79, 95, 105, 113, 114, 126, 130, 135, \dots\}$

$(\text{---} \parallel \text{---}) \cap \{n \mid \gcd(n,56)=1\} = \{9, 15, 25, 39, 57, 65, 71, 79, 95, 113, 135, \dots\}$

$S(f_2)_{prim} \cap \mathbb{P} = \{71, 79, 113, \dots\}$

If $3n = u^2+14v^2 \Rightarrow u \equiv \pm v \pmod 3$, $u = 3x \pm y$, $v = y \Rightarrow n = \dfrac{(3x\pm y)^2+14y^2}{3} = 3x^2 \pm 2xy + 5y^2$

$\boxed{f_3 = 3x^2+2xy+5y^2}$, $f_4 = 3x^2-2xy+5y^2$

$S(f_3)_{prim} (= S(f_4)_{prim}) = \{3, 5, 6, 10, 13, 19, 21, 26, 27, 35, 38, 42, 45, \dots\}$

$(\text{---} \parallel \text{---}) \cap \{n \mid \gcd(n,56)=1\} = \{3, 5, 13, 19, 27, 45, \dots\}$

$S(f_3)_{prim} \cap \mathbb{P} (= S(f_4)_{prim} \cap \mathbb{P}) = \{3, 5, 13, 19, \dots\}$

Congruence conditions (mod 56): $-56 = (-7)\cdot 8$, $\left(\frac{-56}{p}\right) = \left(\frac{-7}{p}\right)\left(\frac{8}{p}\right) = \chi_{-7}(p)\chi_8(p)$ $(p \neq 2,7 \text{ prime})$

$\chi_{-7}: (\mathbb{Z}/7\mathbb{Z})^* \to \{\pm 1\}$, $a \mapsto \left(\frac{a}{7}\right)$, $\chi_{-7}(a) = \begin{cases} 1, & a \equiv 1,2,4 \ (7) \\ -1, & a \equiv 3,5,6 \ (7) \end{cases}$ $\left(\frac{p}{7}\right)$

$\chi_8: (\mathbb{Z}/8\mathbb{Z})^* \to \{\pm 1\}$, $a \mapsto (-1)^{\frac{a^2-1}{8}}$, $\chi_8(a) = \begin{cases} 1, & a \equiv \pm 1 \ (8) \\ -1, & a \equiv \pm 5 \ (8) \end{cases}$

$\chi_{-56} = \chi_{-7}\chi_8 : (\mathbb{Z}/56\mathbb{Z})^* \to \{\pm 1\}$

$\chi_{-56}(a) = 1 \Leftrightarrow \begin{cases} \chi_{-7}(a) = \chi_8(a) = 1 & \Leftrightarrow a \equiv 1,9,15,23,25,39 \pmod{56} \\ \chi_{-7}(a) = \chi_8(a) = -1 & \Leftrightarrow a \equiv 3,5,13,19,27,45 \pmod{56} \end{cases}$

It seems: $\left(S(f_1)_{prim} \cup S(f_2)_{prim}\right) \cap \{n \mid \gcd(n,56)=1\} \overset{?}{=} \{n>0 \mid p \mid n \Rightarrow \chi_{-56}(p)=1,\ \chi_{-7}(n) = \chi_8(n) = 1\}$

$S(f_3)_{prim} (= S(f_4)_{prim}) \cap (\text{---} \parallel \text{---}) \overset{?}{=} \{n>0 \mid p \mid n \Rightarrow \chi_{-56}(p)=1,\ \chi_{-7}(n) = \chi_8(n) = -1\}$

True! But one cannot distinguish $S(f_1)_{prim}$ or $S(f_2)_{prim}$ individually by any congruence condition!

Four classes of (positive definite) forms with $\Delta = -56$: principal class f_1, f_2, f_3, f_4

Two genera, each containing two classes: $\{f_1, f_2\}$, $\{f_3, f_4\}$ — $\{f_1, f_2\}$ principal genus

Here $f_1 \sim f_2$ over $\mathbb{Q}$ ($\Leftarrow f_2$ represents $9 \in \mathbb{Q}^{\times 2}$)

$f_3 \sim f_4$ over $\mathbb{Q}$

Note: $p \neq 2,7$ $p \equiv 1,9,15,23,25,39 \ (56) \Leftrightarrow \begin{cases} p = x^2+14y^2 \text{ or} \\ 2p = x^2+14y^2 \end{cases}$

$p \equiv 3,5,13,19,27,45 \ (56) \Leftrightarrow 3p = x^2+14y^2$

The general picture (for fixed $\Delta \equiv 0,1 \bmod 4$, $\Delta \neq \square$, $\sqrt{\Delta} \notin \mathbb{Z}$)

f, g primitive: $\gcd(a,b,c) = 1$

$f \sim g$ over $\mathbb{Z}$ $\Longrightarrow$ $f \sim g$ over $\mathbb{R}$ and over all $\mathbb{Z}_p$ $\Longrightarrow$ $\forall n \geq 1$ $f, g \pmod n$ represent the same values in $\mathbb{Z}/n\mathbb{Z}$

(f, g are in the same class) — (f, g are in the same genus)

$\Downarrow$ — $\Downarrow$ ($\Uparrow$ if Δ = fundamental)

$f \sim g$ over $\mathbb{Q}$ $\Longleftrightarrow$ (Minkowski–Hasse) — $f \sim g$ over $\mathbb{R}$ and over all $\mathbb{Q}_p$

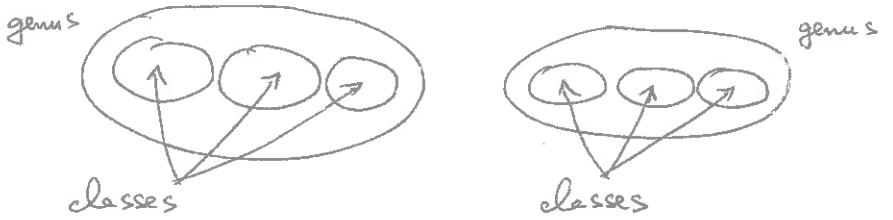
$\Downarrow$ — $\Updownarrow$

f, g represent the same values in $\mathbb{Z}$ — $\forall v \in Pl(\mathbb{Q})$ $\underbrace{(a, -\Delta/a)_v}_{(a,\Delta)_v} = \underbrace{(a', -\Delta/a')_v}_{(a',\Delta)_v}$

$f = ax^2 + bxy + cy^2$, $g = a'x^2 + b'xy + c'y^2$

$f \sim \langle a, -\Delta/a \rangle$ over $\mathbb{Q}$

$g \sim \langle a', -\Delta/a' \rangle$ over $\mathbb{Q}$



Facts: (1) every genus contains the same number of classes

(2) there are 2^{μ} genera ($\mu = |\{\text{primes dividing } \Delta\}| - 1 + \text{small error term}$)

$m \in \mathbb{Z} \setminus \{0\}$:

f represents m over $\mathbb{Z}$ $\Longrightarrow$ f represents m over $\mathbb{R}$ (and over all $\mathbb{Z}_p$) $\Longleftrightarrow$ $\exists f' \in$ the genus of f, f' represents m over $\mathbb{Z}$

$\Downarrow$ — $\Downarrow$ ($\Uparrow$ if Δ = fundamental)

—— " —— $\mathbb{Q}$ $\Longleftrightarrow$ (Legendre) —— " —— $\mathbb{R}$ and all $\mathbb{Q}_p$ $\Longleftrightarrow$ $\forall v \in Pl(\mathbb{Q})$ $(\Delta, am)_v = 1$

Ex: $\Delta = 4 \cdot 34$ — two genera, four classes

$x^2 - 34y^2$

$-x^2 + 34y^2$

(one genus)

$3x^2 + 4xy - 10y^2$

$3x^2 - 4xy - 10y^2$

(another genus)

$x^2 - 34y^2$ represents 1 over $\mathbb{Z}$

$-x^2 + 34y^2$ —— " —— $\mathbb{R}, \mathbb{Q}$ and all $\mathbb{Z}_p$, but not over $\mathbb{Z}$

Rmk: If $f = \sum_{i,j=1}^{n} a_{ij} x_i x_j$, $a_{ij} = a_{ji} \in \mathbb{Z}$ is non-degenerate, indefinite and $n \geq 4$, then:

f represents $m \in \mathbb{Z} \setminus \{0\}$ over $\mathbb{Z}$

$\Updownarrow$

—— " —— all $\mathbb{Z}_p$.

Results of Gauss

Given: $\Delta \in \mathbb{Z}$, $\Delta \equiv 0,1 \pmod 4$, $\sqrt{\Delta} \notin \mathbb{Z}$

(1) $\{ f = ax^2+bxy+cy^2 \mid \Delta(f) = b^2-4ac = \Delta,\ \gcd(a,b,c)=1,\ f \text{ positive definite if } \Delta<0 \}$ is a finite disjoint union of classes $\mathcal{C}$

(2) $f, f' \in \mathcal{C} \Rightarrow f, f'$ represent the same subset of $\mathbb{Z}$

(3) the set of classes $Cl^+(\Delta) = \{\mathcal{C}\}$ has a natural structure of a finite abelian group. Explicitly, if $f \in \mathcal{C} = [f]$ and $f' \in \mathcal{C}' = [f']$, then $f(x,y)\, f'(x',y') = f''(\underbrace{x'', y''}_{\text{Bilinear expressions in } x, x', y, y'})$, $f'' \in \mathcal{C}\mathcal{C}'$

Ex: $(3x^2+2xy+5y^2)(3x'^2+2x'y'+5y'^2) = 2(xx'-2xy'-2yx'-3yy')^2+7(xx'+xy'+yx'-yy')^2$

$$[f_3]^2 = [f_3]\cdot[f_3] = [f_2]$$

$$(3x^2+2xy+5y^2)(3x'^2-2x'y'+5y'^2) = (3xx'-xy'+yx'-5yy')^2 + 14(xy'+yx')^2$$

$$[f_3]\cdot[f_4] = [f_1]$$

f_1 = the principal form, $[f_1]$ = the neutral element of $Cl^+(\Delta)$

$[f_3]^4 = [f_2]^2 = [f_1]$, $\quad Cl^+(-56) \simeq \mathbb{Z}/4\mathbb{Z}$

(4) $\exists$ efficient algorithm (reduction theory) for finding nice representatives of each class $\mathcal{C} \in Cl^+(\Delta)$ and for deciding whether or not f, f' belong to the same class.

(5) $\exists$ subgroup $\underbrace{Cl^+(\Delta)_0}_{\text{the principal genus}} \subset Cl^+(\Delta)$ defined by congruence conditions $\pmod{|\Delta|}$ such that the decomposition of $Cl^+(\Delta)$ into genera $Cl^+(\Delta) = \bigsqcup \underbrace{\mathcal{C}_i\, Cl^+(\Delta)_0}_{\text{the genus of the class } \mathcal{C}_i}$ is given by suitable congruence conditions $\pmod{|\Delta|}$ for the values $\{ f(x,y) \mid \gcd(x,y)=1,\ f \in \text{genus} \}$

(6) $Cl^+(\Delta)_0 = Cl^+(\Delta)^2 = \{ \mathcal{C}^2 \mid \mathcal{C} \in Cl^+(\Delta) \} \Rightarrow$ the group of genera $Cl^+(\Delta)/Cl^+(\Delta)_0 = Cl^+(\Delta)/Cl^+(\Delta)^2$ is of the form $(\mathbb{Z}/2\mathbb{Z})^\mu$

(7) $\mu = |\{ p \text{ prime},\ p \mid \Delta \}| - 1$ (+ small error term)

Everything can be reformulated in terms of arithmetic of the ring $\mathcal{O}_\Delta = \mathbb{Z}\left[\frac{\Delta+\sqrt{\Delta}}{2}\right]$.

The Quadratic Reciprocity Law plays a crucial role here (but it can also be deduced from main results of genus theory).