We start with an observation.

If $Q = [a, b, c]$ represent n, then this means $\exists\ r, s \in \mathbb{Z}$ s.t.

$$Q(r, s) = n.$$

If $t \mid r$ and $t \mid s$ then $t^2 \mid n$ and

$Q(r/t, s/t) = n/t^2$ and Q represents n/t^2.

Defn We say Q properly represents n if $\exists\ r, s \in \mathbb{Z}$, s.t. $(r, s) = 1$ and $Q(r, s) = n$. Such a rep is also called primitive

We want to count different ways a form Q properly represents n

Ie $\#\{(x, y) \in \mathbb{Z}^2 \mid (x, y) = 1 \text{ and } Q(x, y) = n\}$

Here something called the automorphs of Q intervene.

These are exactly the stabilizers of Q

Ie $\Gamma_Q = \{M \in \Gamma \mid M \cdot Q = Q\}$

Ie the change of variables M which leave the form fixed.

ie $Q(x,y) = Q((x,y)M^t) =$

Say $n = Q(r,s)$ then $n = Q((r,s)M^t)$

and we do not want to count these reps different.

Indeed if $D>0$, there are inf many such automorphs and unless we mode out by the action of Γ_Q the set of solns $\{(x,y) \in \mathbb{Z} \mid (x,y)=1, Q(x,y)=n\}$ is infinite.

Note that there are always 2 trivial autom namely $\pm$ identity

ie $x'=x$ $y'=y$ and $x'=-x$, $y'=-y$

For $D<0$ there is in general no other automorphs except in 2 cases, $D=-3,-4$

If $D=-3$ the principal form x^2+xy+y^2 is the only class and has additional automs $x=-y'$ $y=x'+y'$ and $x=x'+y'$ $y=-x'$

and their negatives

If $D=-4$ then principal form is x^2+y^2 additional automorphs $x=y'$, $y=-x'$ and its negative

For $D<0$

Let $w_Q = |T_Q|$, then $w = w_Q = \begin{cases} 2 & \text{if } D<-4 \\ 4 & \text{if } D=-4 \\ 6 & \text{if } D=-3 \end{cases}$

In general we have

Thm 7.5 Let $Q = [a,b,c] \in \mathcal{Q}_D$. Then the automorphs T_Q of Q are in one-to one correspondence with solutions (t,u) of $t^2 - Du^2 = 4$ via

$$(t,u) \longmapsto M_Q = \begin{pmatrix} \frac{t-bu}{2} & -cu \\ au & \frac{t+bu}{2} \end{pmatrix}$$

When $D>0$ these lead to only many solns and $T_Q \cong \mathbb{Z}_2 \times \mathbb{Z}$

For $D=-3$ the 6 solns of $t^2 + 3u^2 = 4$ are

$$(t,u) = \pm \{(1,1), (1,-1), \underbrace{(2,0)}_{t}\}$$

For $D=-4$ there are 4 solns of $t^2 + 4u^2 = 4$ given by

$$(t,u) = \pm \{(0,1), (2,0)\}.$$

For a proof see Zagier's book on quadratic forms.

For the rest we will consider $D<0$ ($a>0$ case of positive def. forms) and define

$$r_{Q,D}(n) := \frac{1}{w} \#\{(x,y)\in\mathbb{Z}^2 \mid (x,y)=1,\ Q(x,y)=n\}$$
$$\text{disc } Q = D$$

and $r_D(n) := \sum_{i=1}^{h_D} r_{Q_i}(n)$ ← Total repn #.

($r_{Q_i}(n)$ = # of primitive reps of n by Q_i)

where $h_D = \left|\left\{[a,b,c] \mid (a,b,c)=1,\ b^2-4ac=D,\ a>0\right\}\right| = |\{Q_1, Q_2, \dots Q_{h_D}\}|$

Clearly $r_{Q,D}(n)$ depends only on the equivalence class of Q. For an individual Q, we do not have a closed formula for $r_{Q,D}(n)$ but there is a closed formula for $r_D(n)$.

Remark: Note that if $R_D(n) := \sum_{i=1}^{h_D} R_{Q_i}(n)$

where $R_Q(n) = \frac{1}{w_D}\#\{(x,y)\in\mathbb{Z}^2 \mid Q(x,y)=n\}$

denote the # of reps of n without the condition $(x,y)=1$ then

$$R_D(n) = \sum_{\substack{t\geq 1 \\ t^2 \mid n}} r_D\left(\frac{n}{t^2}\right)$$

Before we give the formula for $r_D(n)$, we have

Lemma 7.6 If a form $Q(x,y)$ properly represents n then $Q \sim [n,m,\ell]$ for some m,ℓ

Proof. Suppose $Q(r,s)=n$ with $(r,s)=1$. Then $\exists\ t,u$ s.t.

$$\gamma^t = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL_2(\mathbb{Z})$$

Let

$$[A',B',C'] = Q'(x,y) = (\gamma \cdot Q)(x,y) = Q((x,y)\gamma^t)$$

Then $Q' \sim Q$ and

$$Q'(1,0) = Q((1,0)\begin{pmatrix} r & s \\ t & t \end{pmatrix}) = Q(r,s) = n$$

But $Q'(1,0) = A'$ Hence $Q' = [n,*,*]$.

∎

Rmk If Q represents n and $Q \sim Q' = [n,m,\ell]$ then since equivalent forms have the same discriminant $\operatorname{disc} Q = \operatorname{disc} Q'$

$$D = \operatorname{disc} Q = m^2 - 4n\ell = \operatorname{disc} Q'$$

Hence $\boxed{m^2 \equiv D \bmod 4n}$

This gives a <u>necessary condition</u> to test whether any form of disc D can properly represent n. Namely we can check if D is congruent to a square mod $4n$. If not, n cannot be represented

$D = -35$

Ex. $n = 2$ can not be represented by any form of disc $= -35$

Since in this case $4 \cdot n = 8$

and $-35 \equiv 5 \bmod 8$ but 5 is not a square mod 8. ($1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \ (8)$)

$n = 5$, $4n = 20$, $-35 \equiv 5 \bmod 20$

$5 \equiv 5^2 \bmod 20$. In this case $[5, 5, 3] \in \mathcal{Q}_{-35}$ represents 5.

$n = 9$ $4n = 36$, and $-35 \equiv 1 \bmod 36$.

There are at least 2 soln for $m^2 \equiv 1 \bmod 36$

$1^2 \equiv 17^2 \bmod 36$

and there are at least 2 forms $[9, 1, *]$

$[9, 17, *]$

that represent 9.

We also observe that in fact we can improve lemma 7.6 as follows.

Lemma 7.6' If a form Q represents n properly (ie. $\exists\, r,s \in \mathbb{Z}^2$ s.t. $Q(r,s)=n$, $(r,s)=1$) then Q is equivalent to a form $[n,m,\ell]$ where m can be chosen mod $2n$.

Pf We've already seen that if n is properly represented by Q then $Q \sim [n,m',\ell'] = Q'$ for some m', ℓ'.

If we now act by matrix $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ on Q' then we get $Q'' = [n, m'+2nt, *]$.

More precisely

$$Q''(x,y) = Q'\left((x,y)\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}\right) = nx^2 + (m'+2nt)xy + (nt^2 + m't + \ell')y^2$$

Hence $Q \sim Q' \sim Q'' = [n, m'+2nt, *]$

Hence middle coef. m can be chosen in any fixed cong. class rep. mod $2n$ by an app. choice of t ∎

The next thm says that the conditions $m^2 \equiv D \bmod 4n$ and $m \bmod 2n$ are exactly the conditions we need to count the solns in $r_D(n)$ when D is a "fundamental" discriminant.

Defn An integer D is called a fundamental disc if either $D \equiv 1 \bmod 4$, D squarefree or $D \equiv 0 \bmod 4$, $D/4$ squarefree, $\frac{D}{4} \equiv 2 \text{ or } 3 \ (4)$

Exercise: If D is a fundamental discriminant, then any quadratic form of discriminant D is primitive.

Thm 7.7 For $D < 0$ a fundamental discriminant, we have:

$$r_D(n) = \#\{ b \bmod 2n \mid b^2 \equiv D \bmod 4n \}.$$

Proof. For the proof we will use a general fact about a group G acting on 2 sets simultaneously and consider the action of G on the product of 2 sets via diagonal action. More precisely

Proof of Thm 7.7

Let G act on 2 sets X, and Y

$S \subset X \times Y$ s.t. $G.S \subset S$

where action of G on $X \times Y$ is diagonal

ie $g \cdot (x,y) := (g.x, g.y)$

We say $(x,y), (x',y') \in S$ are equivalent if

$(x',y') = (gx, gy)$

In particular its first components are G-equivalent

We can look at the set of orbits S/G

by first describing X/G and then

asking which elts of S/G has $[x] \in X/G$ as the first component.

Two such pairs $(x,y), (x,y')$ are then equivalent if $y' = gx$ and $gx = x$. Note this means g is in fact in G_x

These orbits are then one to one correspondence with the orbits of $Y_x := \{y \in Y \mid (x,y) \in S\}$ under the action of $G_x = \{g \in G \mid gx = x\}$, stabilizer of x in G. (Exercise)

Hence $$|S/G| = \sum_{x \in X/G} |Y_x/G_x|$$

Similarly interchanging the roles of x and y gives

$$|S/G| = \sum_{y \in Y/G} |X_y/G_y| = \sum_{x \in X/G} |Y_x/G_x|$$

We now apply this principle in the following setting.

Let $G = SL_2(\mathbb{Z}) = \Gamma$

$$X = Q_D^* = \{Q = Q(x,y) = ax^2 + bxy + c \mid \underset{\text{primitive}}{} \; b^2 - 4ac = D, \; a > 0\}$$

$$Y = \{z = (x,y) \in \mathbb{Z}^2 \mid \gcd(x,y) = 1\}$$

$$S = \{(Q, z) \in X \times Y \mid Q(z) = n\}$$

Then $X/G = Q_D^*/\Gamma$ is the equivalence classes of primitive forms of disc D.

Let $Q \in X$, $Y_Q = \{z = (x,y) \in Y \mid Q(z) = Q(x,y) = n\}$

ie $\gcd(x,y) = 1$

$= \{$Proper representations of n by $Q\}$

$G_Q = \{g \in \Gamma \mid gQ = Q\}$ = automorphs of Q

Hence $|Y_Q/G_Q|$ = # of inequivalent primitive reps of n by Q.
$= r_Q(n)$

So $|S/G| = \sum_{Q \in \mathcal{Q}_{D/\Gamma}} r_Q(n) = r_D(n)$
$= \sum_{x \in X/G} Y_x/G_x$

On the other hand we can also use $|S/G| = \sum_{Y \in Y/G} (X_y/G_y)$

In this case $Y/\Gamma \cong Y/G$ is just 1 orbit $= \{[(1,0)]\}$

w/ rep $z = (1,0)$ since if $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$

then $(1,0)g^t = (1\ 0)\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} = (\alpha\ \gamma)$

$\gcd(\alpha, \gamma) = 1$ since $g \in \Gamma$.

and conversely any $(\alpha, \gamma) \in \mathbb{Z}^2$ w/ $\gcd(\alpha, \gamma) = 1$
$\exists\ \delta, \beta$ s.t. $g^{-1} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma$ and $(\alpha\ \gamma)g^{-t} = (1,0)$

For $z = (1\ 0)$, $G_z = \{ g \in \Gamma \mid (1\ 0)g^t = (1,0) \}$

$= \left\{ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \mid t \in \mathbb{Z} \right\}$

since $(1\ 0)\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = (1\ 0)$ and check $(1\ 0)g^t = (1\ 0)$

$\Rightarrow g$ is of the form $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$.

7.34

$$X_z = \{ x \in X \mid (x, z) \in S \}$$

$$= \{ Q \in Q_D \mid Q(z) = n \}$$

For $z = (1, 0)$, $X_z = \{ Q = [a, b, c] \in Q_D \mid Q(1,0) = n \}$

$$= \{ Q = [a, b, c] \mid \begin{matrix} a = n \\ b^2 - 4nc = D \end{matrix} \}$$

But $b^2 - 4nc = D \Rightarrow b^2 \equiv D \bmod 4n$.

Hence $X_{(f,b)} = \{ nx^2 + bxy + \underbrace{\frac{b^2 - D}{4n}}_{= c} y^2 \mid b^2 \equiv D \bmod 4n \}$

$$= \{ [n, b, c] \mid b^2 \in \mathbb{Z},\ b^2 \equiv D \bmod 4n \}$$

The action of $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \in G_z$ on $[n, b, c]$

is $[n, b + 2nt, c^*]$ (Note once a, b is fixed, c is fixed by $b^2 - 4ac = D$)

Hence $\left| X_z / G_z \right| = \# \{ b \bmod 2n \mid b^2 \equiv D \bmod 4n \}$

Hence $\underbrace{\left| S / G \right| = \sum_{Q \in Q_D / \Gamma} \left| X_Q / G_Q \right| = \sum_{Q \in Q_D / \Gamma} r_Q(n)}_{\text{First part}}$

$$= r_D(n) = \sum_{z \in Y / G} \left| X_z / G_z \right|$$

$$= \left| X_{(1,0)} / G_{(1,0)} \right| -$$

$$= \{ b \in \mathbb{Z} \mid b \bmod 2n,\ b^2 \equiv D \bmod 4n \}$$