Lemma 2: Let $n \geq 1$ be an integer and $(n,d)=1$. Then

$$\#\{l : 0 \leq l \leq 2n-1,\ l^2 \equiv d \pmod{4n}\} = \sum_{\substack{m \mid n \\ m \text{ squarefree}}} \left(\frac{d}{m}\right)$$

Proof: Note: $(l+2n)^2 = l^2 + 4nl + 4n^2 \equiv d \pmod{4n}$

It suffices to show:

$$\#\{l \in \mathbb{Z}/4n\mathbb{Z} : l^2 \equiv d \pmod{4n}\} = 2 \sum_{\substack{m \mid n \\ m \text{ squarefree}}} \left(\frac{d}{m}\right)$$

Write $4n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ with $\begin{cases} p_i \text{ distinct primes} \\ p_1 = 2 \end{cases}$

By Chinese Remainder Theorem:

$$\#\{l \in \mathbb{Z}/4n\mathbb{Z} : l^2 \equiv d \pmod{4n}\}$$
$$= \prod_{j=1}^{r} \#\{l \in \mathbb{Z}/p_j^{\alpha_j}\mathbb{Z} : l^2 \equiv d \pmod{p_j^{\alpha_j}}\}$$

Claim: let p_j be odd, then

$$\#\{l \in \mathbb{Z}/p_j^{\alpha_r}\mathbb{Z} : l^2 \equiv d \bmod p_j^{\alpha_j}\} = 1 + \left(\frac{d}{p_j}\right)$$

$(n,d)=1 \quad p_j \mid n$ and p_j odd $\Rightarrow (p_j, d) = 1$

$$\Rightarrow \left(\frac{d}{p_j}\right) = \begin{cases} 1 & \text{if } l^2 \equiv d \pmod{p_j} \text{ has a solution} \\ -1 & \text{if } l^2 \equiv d \pmod{p_j} \text{ has no solution.} \end{cases}$$

① If $\left(\frac{d}{p_j}\right) = -1$, $1 + \left(\frac{d}{p_j}\right) = 0$

$\ell^2 \equiv d \pmod{p_j}$ has no solution for $\ell \in \mathbb{Z}/p\mathbb{Z}$

$\Rightarrow \ell^2 \equiv d \pmod{p_j^{\alpha_j}}$ has no solution. for $\ell \in \mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}$.

$\Rightarrow \#\{\ell \in \mathbb{Z}/p_j^{\alpha_j}\mathbb{Z} : \ell^2 \equiv d \pmod{p_j^{\alpha_j}}\} = 0$.

$\Rightarrow$ LHS = RHS.

② If $\left(\frac{d}{p_j}\right) = 1$, then $1 + \left(\frac{d}{p_j}\right) = 2$.

Fact: let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial.

Suppose that $f(x_0) \equiv 0 \pmod{p}$ for some $x_0 \in \mathbb{Z}/p\mathbb{Z}$

and $f'(x_0) \not\equiv 0 \pmod{p}$. Then for any p^α

$f(x) \equiv 0 \pmod{p^\alpha}$ has a solution in $\mathbb{Z}/p^\alpha\mathbb{Z}$

This is a weak version of "Hensel's Lemma."

In our case, set $f(x) = x^2 - \ell$. $f'(x) = 2x$

$\left(\frac{d}{p_j}\right) = 1 \Rightarrow f(x) \equiv 0 \pmod{p_j}$ has a solution x_0

$f'(x_0) \not\equiv 0 \pmod{p} \Rightarrow f(x) \equiv 0 \mod p_j^{\alpha_j}$ has a solution.

A direct calculation show: if $f(x_0) \equiv 0 \mod p_j^{\alpha_j}$

$f(p_j^{\alpha_j} - x_0) \equiv 0 \; p_j^{\alpha_j}$

$f(x) = x^2 - \ell$.

We also show: they are the only possibilities.

Assume that $a^2 \equiv \ell \bmod p^\alpha$ $\quad b^2 \equiv \ell \bmod p^\alpha$

$$(a+b)(a-b) \equiv a^2 - b^2 \equiv 0 \pmod{p^\alpha}$$

$$\Rightarrow p^\alpha \mid (a+b)(a-b).$$

Notice that we can choose: $\quad a, b \in \{0, 1, \cdots p^\alpha - 1\}$

and $\quad (a,p), (b,p) = 1.$

This will force: $\quad a+b = p^\alpha.$

Therefore, there are at most 2 solutions.

Next, we consider $p_1 = 2$, $\quad 4n = 2^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \Rightarrow \alpha_1 \geq 2.$

Fact:

$$\#\{\ell \in \mathbb{Z}/2^{\alpha_1}\mathbb{Z} : \ell^2 \equiv d \pmod{2^{\alpha_1}}\} = \begin{cases} 2 & \text{if } \alpha_1 = 2 \\ 2\left(1+\left(\frac{d}{2}\right)\right) & \alpha_1 \geq 3. \end{cases}$$

Therefore: we showed:

$$\#\{\ell \in \mathbb{Z}/4n\mathbb{Z} : \ell^2 \equiv d \pmod{4n}\}$$

$$= \prod_{\substack{p \mid n \\ p \text{ odd}}} \left(1 + \left(\frac{d}{p}\right)\right) \times \begin{cases} 2 & \text{if } (n,2) = 1. \\ 2\left(1+\left(\frac{d}{2}\right)\right) & \text{if } (n,2) > 1. \end{cases}$$

$$= 2 \prod_{p \mid n} \left(1 + \left(\frac{d}{p}\right)\right)$$

Suppose that n has primes $p_1, \cdots p_r$

$$\prod_{p|n}\left(1+\left(\frac{d}{p}\right)\right) = 1 + \left(\frac{d}{p_1}\right) + \left(\frac{d}{p_2}\right) + \cdots \left(\frac{d}{p_r}\right)$$
$$+ \left(\frac{d}{p_1p_2}\right) + \left(\frac{d}{p_1p_3}\right) + \cdots \quad \left(\frac{d}{p_r p_{r-1}}\right)$$
$$+ \cdots$$
$$+ \left(\frac{d}{p_1 \cdots p_r}\right)$$

This contains all squarefree divisors of n.

$$= \sum_{\substack{m|n \\ m \text{ squarefree}}} \left(\frac{d}{m}\right) \qquad \square$$

Recall:

Lemma 1: Let $d<0$ be a fundamental discriminant. $(n,d)=1$

Then there is a w-to-1 map from:

$$M_1 = \{ \langle Q, x, y \rangle : Q \in S_d, \ Q(x,y) = n, \ (x,y) \}$$

and

$$M_2 = \{ l : 0 \le l \le 2n-1, \ l^2 \equiv d \pmod{4n} \}$$

Theorem: Let $n \geq 1$ be an integer, and $(n,d)=1$. Then

$$R(n;d) = w \sum_{m|n} \left(\frac{d}{n}\right)$$

Proof of Theorem: Recall:

$$\begin{aligned}
R^*(n;d) &= \sum_{Q \in S_d} R_Q(n) \\
&= \#\{\langle Q, x, y\rangle,\ Q \in S_d,\ Q(x,y)=n,\ (x,y)=1\} \\
&= \# M_1 \qquad \text{Lemma 1} \\
&= w \cdot \# M_1 \qquad \text{Lemma 2.} \\
&= w \cdot \sum_{\substack{m \mid n \\ m \text{ squarefree}}} \left(\frac{d}{m}\right)
\end{aligned}$$

$$\Rightarrow \quad R^*(n;d) = w \cdot \sum_{\substack{m \mid n \\ m \text{ squarefree}}} \left(\frac{d}{m}\right)$$

Claim: for each $Q \in S_d$, $\quad R_Q(n) = \sum_{\ell^2 \mid n} R_Q^*\left(\frac{n}{\ell^2}\right)$

We construct a bijection:

$$M_1 = \{(x,y) : Q(x,y) = n\}$$

and

$$M_2 = \bigsqcup_{\ell^2 \mid n} \left\{(x,y) : Q(x,y) = \frac{n}{\ell^2},\ (x,y)=1\right\}$$

Take $(x,y) \in M_1$, set $l = (x,y)^{>0}$. Then

$$Q\left(\frac{x}{l}, \frac{y}{l}\right) = \frac{n}{l^2} \quad \text{and} \quad \left(\frac{x}{l}, \frac{y}{l}\right) = 1.$$

Therefore, $F: M_1 \longrightarrow M_2$

$$F: (x,y) \longmapsto \left(\frac{x}{(x,y)}, \frac{y}{(x,y)}\right)$$

This is an injection, as (x,y) is unique.

$(a,b)=1$.

Next, take $(a,b) \in M_2$, then $Q(a,b) = \frac{n}{l^2}$ for some l.

Then $(al, bl) \in M_1$ and $F(al, bl) = (a,b)$

This implies: $\# M_1 = \# M_2$, i.e.

$$R_Q(n) = \sum_{l^2 | n} R_Q^*\left(\frac{n}{l^2}\right) \quad \text{for any } Q \in S_d$$

$$\Rightarrow R(n;d) = \sum_{Q \in S_d} R_Q(n) = \sum_{Q \in S_d} \sum_{l^2 | n} R_Q^*\left(\frac{n}{l^2}\right)$$

$$= \sum_{l^2 | n} \sum_{Q \in S_d} R_Q^*\left(\frac{n}{l^2}\right) = \sum_{l^2 | n} R^*\left(\frac{n}{l^2}; d\right)$$

$$= w \cdot \sum_{l^2 | n} \sum_{\substack{m | \frac{n}{l^2} \\ m \text{ squarefree}}} \left(\frac{d}{m}\right)$$

Note that $\left(\frac{d}{m}\right) = \left(\frac{d}{m}\right) \underbrace{\left(\frac{d}{l}\right)^2}_{1} = \left(\frac{d}{m}\right) \cdot \left(\frac{d}{l^2}\right) = \left(\frac{d}{ml^2}\right)$

$$\Rightarrow R(n;d) = w \sum_{\ell^2 | n} \sum_{\substack{m | \frac{n}{\ell^2} \\ m \text{ square free}}} \left(\frac{d}{m\ell^2}\right)$$

Recall, we can write $n = n_0 \cdot n_1^2$ s.t. n_0 is squarefree.

Then $\ell^2 | n \iff \ell^2 | n_1^2 \iff \ell | n_1$

$m | \frac{n}{\ell^2}$, m squarefree $\iff m | n_0$.

$\Rightarrow$ There is a bijection between:

$$\{(\ell, m) : \ell | n_1, \; m | n_0\} \longrightarrow \{ y : y | n \}$$

$$\Rightarrow \sum_{\ell^2 | n} \sum_{\substack{m | \frac{n}{\ell^2} \\ m \text{ square free}}} \left(\frac{d}{m\ell^2}\right) = \sum_{y | n} \left(\frac{d}{y}\right)$$

$$\Rightarrow R(n;d) = w \sum_{y | n} \left(\frac{d}{y}\right)$$ 口.

Class number formula:

We study:

$$G_d(N) = \frac{1}{wN} \sum_{\substack{1 \le n \le N \\ (n,d)=1}} R(n;d) = \frac{1}{N} \sum_{\substack{1 \le n \le N \\ (n,d)=1}} \sum_{m | n} \left(\frac{d}{m}\right)$$

$$\mathrm{I}: \quad \lim_{N\to\infty} G_d(N) = \frac{\phi(|d|)}{w|d|} \frac{2\pi}{|d|^{\frac{1}{2}}} h(d)$$

$$\mathrm{II}: \quad \lim_{N\to\infty} G_d(N) = \frac{\phi(d)}{|d|} L(1, \chi_d)$$

$$\mathrm{I} + \mathrm{II} \Rightarrow \quad L(1, \chi_d) = \frac{2\pi}{w\sqrt{|d|}} h(d)$$