Each orbit (corr. to L) is compact because it is the image of the compact set $GL_2(\mathbb{Z}_p)$ under the cont. map η_f (where $f \in V^{\max}(\mathbb{Z}_p)$ corr. to L). Since there are only fin. many such L (see PSet 6), this implies that $V^{\max}(\mathbb{Z}_p)$ is compact.

Since the Jacobian of η_f is invertible everywhere, η_f is an open map. $\Rightarrow$ The orbit (= image of the open set $GL_2(\mathbb{Z}_p)$) is open.

$\Rightarrow V^{\max}(\mathbb{Z}_p)$ is open.

Note: A subset A of $\mathbb{Z}_p^n$ is compact and open if and only if A is the preimage of some subset A' of $(\mathbb{Z}/p^e\mathbb{Z})^n$ for some $e \geq 0$.
("Whether $x \in A$ depends only on $x \bmod p^e$.")

Pf "$\Rightarrow$" Since sets of the form $x + p^e \cdot \mathbb{Z}_p^n$ form a basis of open sets, A can be covered by sets of this form. Since A is cpt., it can be covered by finitely many.

"$\subseteq$" The projection $\mathbb{Z}_p^n \longrightarrow (\mathbb{Z}/p^e\mathbb{Z})^n$ is continuous. Any A' is open and closed.

$\Rightarrow$ $A \subseteq \mathbb{Z}_p^n$ open and closed

$\mathbb{Z}_p^n$ compact $\Downarrow$

A compact

□!

$\Rightarrow$ Whether $f \in V(\mathbb{Z}_p)$ lies in $V^{\max}(\mathbb{Z}_p)$ only depends on $f \bmod p^{e_p}$ for some fixed e_p. The volume $\mathrm{vol}(V^{\max}(\mathbb{Z}_p))$ is the fraction of residue classes belonging to $V^{\max}(\mathbb{Z}_p)$.

Step 6: "Almost all $f \in \mathcal{F}_T' \cap V(\mathbb{Z})$ are irreducible":

$$\#\left(\mathcal{F}_T' \cap \left(V(\mathbb{Z}) \setminus V^{\text{irred}}(\mathbb{Z})\right)\right) = o(T) \quad \text{for } T \to \infty$$

f reducible over $\mathbb{Z}$

$\Rightarrow$ f reducible over $\mathbb{Z}_p$ $\forall p$

$\Rightarrow$ f corresponds to a product of ≥ 2 field ext. of $\mathbb{Q}_p$ (not integral domain) $\forall p$

$\Leftrightarrow$ f doesn't corr. to a field ext. of $\mathbb{Q}_p$ $\forall p$

$\Rightarrow$ f doesn't corr. to the unramified cubic field ext. $L_p = \mathbb{Q}_p(\sqrt[3]{p^3-1})$ of $\mathbb{Q}_p$ $\forall p$

$\Leftrightarrow$ $f \notin$ ($GL_2(\mathbb{Z}_p)$-orbit in $V^{\max}(\mathbb{Z}_p)$ corr. to L_p). $\forall p$.

Let $M \geq 2$.

$$\Rightarrow \#\left(\mathcal{F}_T' \cap \left(V(\mathbb{Z}) \setminus V^{\text{irred}}(\mathbb{Z})\right)\right) \leq \#\left\{f \in \mathcal{F}_T' \cap V(\mathbb{Z}) \,\middle|\, f \notin (\text{orbit corr. to } L_p)\ \forall p \leq M\right\}$$

In step 5, we've seen that the orbit corr to L_p is a p-adic open subset of $V^{\max}(\mathbb{Z}_p)$ of volume

$$\text{vol}(\text{orbit corr. to } L_p) = \frac{|D_{L_p}|^{\mathbb{Q}_p}|}{\#\,\text{Aut}(L_p)} \cdot (1-p^{-2})(1-p^{-1})$$

$$= \frac{1}{3} \cdot (1-p^{-2})(1-p^{-1}).$$

$\Rightarrow$ By applying step 4 to every residue class mod $\prod_{p \le M} p^{e_p}$, you see that

$$\#\{f \in \mathcal{F}_T' \cap U(\mathbb{Z}) \mid f \notin (\text{orbit corr. to } \Lambda_p)\ \forall p \le M\}$$

$$\underset{M}{\sim} \operatorname{vol}(\mathcal{F}_T') \cdot \prod_{p \le M} \left(1 - \operatorname{vol}(\text{orbit corr. to } \Lambda_p)\right)$$

$$= \frac{1}{3} \zeta(2) \cdot T \cdot \prod_{p \le M} \Big(1 - \underbrace{\tfrac{1}{3}(1-p^{-2})(1-p^{-1})}_{\longrightarrow \frac{1}{3} \text{ for } p \to \infty}\Big)$$

But $\prod_{p \le M} \left(1 - \frac{1}{3}(1-p^{-2})(1-p^{-1})\right) \longrightarrow 0$ for $M \to \infty$.

Step 7: "Sieve for mass. esst."

$$\#(\mathcal{F}_T^1 \cap \mathcal{V}^{irred,mass}(\mathbb{Z})) \sim \frac{1}{3\zeta(3)} \cdot T$$

Remember that

$$f \in \mathcal{V}^{mass}(\mathbb{Z})$$

$$\Leftrightarrow \quad f \in \mathcal{V}^{mass}(\mathbb{Z}_p) \quad \forall p$$

Let $M \geq 2$.

$$\Rightarrow 0 \leq \#\{ f \in \mathcal{F}_T^1 \cap \mathcal{V}^{irred}(\mathbb{Z}) : f \in \mathcal{V}^{mass}(\mathbb{Z}_p) \; \forall p \leq M\}$$

main term $\rightarrow$

$$- \#(\mathcal{F}_T^1 \cap \mathcal{V}^{irred,mass}(\mathbb{Z}))$$

$$\leq \#\{f \in \mathcal{F}_T^1 \cap \mathcal{V}^{irred}(\mathbb{Z}) : f \notin \mathcal{V}^{mass}(\mathbb{Z}_p \text{ for some } p > M\}$$

error term $\rightarrow \leq \sum_{p > M} \#\{f \in \mathcal{F}_T^1 \cap \mathcal{V}^{irred}(\mathbb{Z}) : f \notin \mathcal{V}^{mass}(\mathbb{Z}_p)\}$.

By step 4 and the CRT,

$$\#\{f \in \mathcal{F}_T^1 \cap \mathcal{V}^{irred}(\mathbb{Z}) : f \in \mathcal{V}^{mass}(\mathbb{Z}_p) \; \forall p \leq M\}$$

$$\underset{M}{\sim} \mathrm{vol}(\mathcal{F}_T^1) \cdot \prod_{p \leq M} \mathrm{vol}(\mathcal{V}^{mass}(\mathbb{Z}_p))$$

$$= \frac{1}{3}\zeta(2)\cdot T \cdot \prod_{p\le M}(1-p^{-3})(1-p^{-2})$$

↑ step 2,5

But

$$\frac{1}{3}\zeta(2)\cdot\prod_{p\le M}(1-p^{-3})(1-p^{-2}) \xrightarrow[M\to\infty]{} \frac{1}{3\zeta(3)}.$$

By step 8, we have

$$\sum_{p>M} \#\left\{f\in \mathcal{F}_T' \cap \mathcal{V}^{\text{irred}}(\mathbb{Z}) : f\notin \mathcal{V}^{\max}(\mathbb{Z}_p)\right\}$$

$$\ll \sum_{p>M}\frac{T}{p^2} \ll \frac{T}{M} = o_{M\to\infty}(T).$$

Step 8: $\#\left(GL_2(\mathbb{Z})\backslash\left\{f\in \mathcal{V}^{\text{irred}}_{0\neq|\text{disc}|\le T}(\mathbb{Z}) \mid f\notin \mathcal{V}^{\max}(\mathbb{Z}_p)\right\}\right)$

$$\ll \frac{T}{p^2}.$$

↑ doesn't depend on T, p

Claim 1 Let S be a nondeg. cubic eset. of $\mathbb{Z}$ which is not maximal at p. Then, S is a subset. of some cubic eset. S' of $\mathbb{Z}$

of <u>type I</u>: $S/\mathbb{Z} = p \cdot (S'/\mathbb{Z})$:

if (θ_1', θ_2') is a basis of $S'/\mathbb{Z}$, then $(p\theta_1', p\theta_2')$ is a basis of $S/\mathbb{Z}$.

$(\Rightarrow [S' : S] = p^2)$

of <u>type II</u>: there is a basis (θ_1', θ_2') of $S'/\mathbb{Z}$ such that $(p\theta_1', \theta_2')$ is a basis of $S/\mathbb{Z}$ and the cubic form $f' \in V(\mathbb{Z})$ corr. to $(S', (\theta_1', \theta_2'))$ is not divisible by p.

$(\Rightarrow [S' : S] = p)$.

<u>Pf</u> We know that S is a subset. of some cubic eset. S' of $\mathbb{Z}$ of index p^k for some $k \geq 1$. Let (θ_1, θ_2) of $S/\mathbb{Z}$ and let (θ_1', θ_2') of $S'/\mathbb{Z}$. We obtain a base change matrix $M \in M_2(\mathbb{Z}) \cap GL_2(\mathbb{Q})$ sending θ_1' to θ_1 and θ_2' to θ_2, with

$|\det(M)| = [S' : S] = p^k$.

We can put M in Smith normal form:

$M = A \begin{pmatrix} p^r & 0 \\ 0 & p^s \end{pmatrix} B$ with $A, B \in GL_2(\mathbb{Z})$ and $r \geq s \geq 0$. The matrices A, B corr. to changing the bases $(\Theta_1, \Theta_2), (\Theta_1', \Theta_2')$.

$\rightsquigarrow$ W.l.o.g. $A = B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so $M = \begin{pmatrix} p^r & 0 \\ 0 & p^s \end{pmatrix}$.

Note $r+s = k \geq 1$.

Let $(S, (\Theta_1, \Theta_2))$ corr. to $f \in V(\mathbb{Z})$.

$$\| \\ aX^3 + bX^2Y + cXY^2 + dY^3$$

$\Rightarrow (S', (\Theta_1', \Theta_2'))$ corr. to $M^{-1} f \in V(\mathbb{Z})$

$$\| \\ p^{-2r+s} aX^3 + p^{-r} bX^2Y + p^{-s} cXY^2 + p^{r-2s} dY^3$$

$\Rightarrow p^{-2r+s} a, p^{-r} b, p^{-s} c, p^{r-2s} d \in \mathbb{Z}$

If $p^{-1} a, p^{-1} b, p^{-1} c, p^{-1} d \in \mathbb{Z}$, we could take $r = s = 1$, so $\Theta_1 = p\Theta_1'$, $\Theta_2 = p\Theta_2'$ (type I).

Assume not. $\Rightarrow$ We can't have $r = s \geq 1$.

$\Rightarrow r \geq s+1 \geq 1$. $\Rightarrow p^{-2} a, p^{-1} b, c, pd \in \mathbb{Z}$.

$\rightsquigarrow$ We could take $r = 1$, $s = 0$, so

$\Theta_1 = p\Theta_1'$, $\Theta_2 = \Theta_2'$. (type II) — (claim 1) □

<u>Claim 2</u> For fixed p, any nondeg. cubic ext. S' of $\mathbb{Z}$

has a) exactly 1 subext. S of type I (and index p^2)

b) at most 3 subext. S of type II (and index p).

<u>Pf</u> a) clear

b) The subext. S depends on the choice of basis (θ_1', θ_2'), but it only depends on $\theta_1' \bmod \theta_2'$ and $\theta_2' \bmod p \cdot \theta_1'$.

Let $f' \in V(\mathbb{Z}_p)$ corr. to $(S', (\theta_1', \theta_2'))$.
$$f' = aX^3 + \dots + dY^3$$

$$\Rightarrow \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} f' \in V(\mathbb{Z}_p) \text{ corr. to } (S, (\theta_1, \theta_2))$$
$$= p^2 a X^3 + p b X^2 Y + c X Y^2 + p^{-1} d Y^3$$

$$\Rightarrow 0 \equiv d \equiv f'(0,1) \bmod p.$$

The cubic form f' has at most 3 zeroes in $\mathbb{P}^1(\mathbb{F}_p)$ (corr. to valid choices of θ_2'.)

□ (Claim 2)

(cf. section 3 of Bhargava, Shankar, Tsimerman).

This implies step 8:

$$\#\left(GL_2(\mathcal{O}) \setminus \left\{ f \in \mathcal{V}^{\text{irred}}_{0 \neq |\mathrm{disc}| \leq T} (\mathcal{O}) \,\middle|\, f \notin \mathcal{V}^{\text{mase}}(\mathcal{O}_p) \right\}\right)$$

$$\leq 1 \cdot \#\left(GL_2(\mathcal{O}) \setminus \left\{ f \in \mathcal{V}^{\text{irred}}_{\substack{0 \neq |\mathrm{disc}| \leq T \\ p^4 \in \mathrm{index}\, p^2}} (\mathcal{O}) \right\}\right) \quad \text{(type I)}$$

$$+ 3 \cdot \#\left(GL_2(\mathcal{O}) \setminus \left\{ f \in \mathcal{V}^{\text{irred}}_{\substack{0 \neq |\mathrm{disc}| \leq T \\ p^2 \in \mathrm{index}\, p}} (\mathcal{O}) \right\}\right) \quad \text{(type II)}$$

$$\ll \frac{T}{p^4} + \frac{T}{p^2} \ll \frac{T}{p^2}.$$

$\uparrow$ steps 2, 4

$\Rightarrow$ This finishes the proof of the "big goal" Theorem!!!

$\square$