Step 6 Show $\sum_{f\in V^{a\neq 0}(\mathbb{Z})\cap V^m(\mathbb{Z})} \alpha_T(f) \sim \prod_p \omega_p \cdot V \cdot T$.

Recall that $V^m(\mathbb{Z}) = \{f\in V(\mathbb{Z}) \mid f\in V^m(\mathbb{Z}_p)\ \forall p\}$.

⇝ We use a sieve (with step 3). This immediately shows "$\leq$".

For "$\geq$", the only difficulty is showing the following uniformity estimate:

Thm 15.5.9 For any T, p,

$$\sum_{\substack{f\in V(\mathbb{Z})\\ f\notin V^m(\mathbb{Z}_p)}} \alpha_T(f) \ll \frac{T}{p^2}$$

where the constant is independent of T and p.

Note If $f\in V(\mathbb{Z}_p)$, $f\notin V^m(\mathbb{Z}_p)$, then $p^2 \mid \mathrm{disc}(f)$.

Lemma 15.5.10 Let L be an étale cubic $\mathbb{Q}_p$-algebra and $S\subseteq \mathcal{O}_L$ a cubic ext. of $\mathbb{Z}_p$.

If $S\neq \mathcal{O}_L$, then S is a subext. of some cubic ext.

$S \subsetneq S' \subseteq \mathcal{O}_L$

of type I: if (θ_1', θ_2') is a $\mathbb{Z}_p$-basis of $S'/\mathbb{Z}_p$ then $(p\theta_1', p\theta_2')$ is a $\mathbb{Z}_p$-basis of $S/\mathbb{Z}_p$. $(\Rightarrow [S':S]=$

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

Lemma 15.5.10

$=\{f \in V(\mathbb{Q}_p)$ irred. over $\mathbb{Q}_p\}$

Consider an orbit $GL_2(\mathbb{Z}_p)f$ in $V^i(\mathbb{Z}_p)$ with $f \notin V^m(\mathbb{Z}_p)$.
One of the following holds:

a) $p \mid f$

b) $p \nmid f$, but $GL_2(\mathbb{Z}_p)f = GL_2(\mathbb{Z}_p)\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} f'$

for some $f' \in V^i(\mathbb{Z}_p)$. [f, f' corr. to ext. S, S' of $\mathbb{Z}_p$ with $S \subsetneq S'$

index p^2 in case a), index p in case b)

<u>Pf</u> Let f corr. to the ext. S of $\mathbb{Z}_p$ and the ext. L of $\mathbb{Q}_p$.

$\Rightarrow S \subsetneq \mathcal{O}_L$.

Let $\mathcal{O}_L$ corr. to the cubic form $f'' \in V^i(\mathbb{Z})$.

Since $S \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = L = \mathcal{O}_L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, we have $f = M f''$

for some $M \in GL_2(\mathbb{Q}_p)$ (a base change matrix from $\mathcal{O}_L/\mathbb{Z}_p$ to $S/\mathbb{Z}_p$).

Since $S \subseteq \mathcal{O}_L$, we have $M \in M_{2\times 2}(\mathbb{Z}_p)$. (I)

Since $S \neq \mathcal{O}_L$, we have $M \notin GL_2(\mathbb{Z}_p)$, so $\det(M) \notin \mathbb{Z}_p^\times$. (II)

Only the $GL_2(\mathbb{Z}_p)$-orbits of f and f'' matter, so we can (w.l.o.g.) multiply M by elements of $GL_2(\mathbb{Z}_p)$ on the left and on the right (independently) to put M into <u>Smith normal form</u>: $M = \begin{pmatrix} p^r & 0 \\ 0 & p^s \end{pmatrix}$ with $r \geq s$.

(I) $\Rightarrow s \geq 0$.

(II) $\Rightarrow r+s \neq 0$.

Assume $p \nmid f$.

$\Rightarrow$ We can't have $r = s \geq 1$ because then $\mathcal{V}(\mathbb{Z}_p) \ni f'' = M^{-1} f = p^{-r} \cdot f$.

Hence, $r \geq s+1$.

Write $f = aX^3 + bX^2Y + cXY^2 + dY^3$.

$\Rightarrow \mathcal{V}(\mathbb{Z}_p) \ni f'' = M^{-1} f = p^{-2r+s} aX^3 + p^{-r} bX^2Y + p^{-s} cXY^2 + p^{r-2s} dY^3$

$\Rightarrow p^{-2} a, p^{-1} b \in \mathbb{Z}_p$.

$\Rightarrow \underbrace{\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}^{-1} f}_{=: f'} \in \mathcal{V}(\mathbb{Z}_p)$. $\square$

<u>Cor 15.5.11</u>

If moreover $f \in \mathcal{V}^i(\mathbb{Z})$, then

a) $p \mid f$ or

b) $p \nmid f$, but $GL_2(\mathbb{Z}) f = GL_2(\mathbb{Z}) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} f'$ for some $f' \in \mathcal{V}(\mathbb{Z})$.

<u>Pf</u> a) clear

b) We know

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}^{-1} M f \in \mathcal{V}(\mathbb{Z}_p) \text{ for some } M \in GL_2(\mathbb{Z}_p).$$

We can multiply M on the left by an element of the form $\begin{pmatrix} 1 & 0 \\ 0 & \varepsilon \end{pmatrix} \in GL_2(\mathbb{Z}_p)$ (which commutes with $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$!) to make $\det(M) = 1$. There is some $M' \in SL_2(\mathbb{Z})$ such that $M' \equiv M \bmod p^2$. Then, $Mf \equiv M'f \bmod p^2$ implies that we also have $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}^{-1} M' f \in \mathcal{V}(\mathbb{Z})$. $\square$

Pf of Thm 15.5.9

For case a),

$$\sum_{\substack{f\in V^i(\mathbb{Z})\\ p\mid f}} \alpha_T(f) \underset{f=pf'}{=} \sum_{f'\in V^i(\mathbb{Z})} \underbrace{\alpha_T(pf')}_{\alpha_{T/p^4}(f')} \ll \frac{T}{p^4} \text{ by step 3.}$$

For case b):

<u>Claim</u> For each $GL_2(\mathbb{Z})$-orbit $GL_2(\mathbb{Z})f'$ in $V(\mathbb{Z})$ with $p\nmid f'$ for $f'\in B$, there are at most 3 $GL_2(\mathbb{Z})$-orbits A such that $A = GL_2(\mathbb{Z})\begin{pmatrix}p&0\\0&1\end{pmatrix}f'$ for some $f''\in GL_2(\mathbb{Z})f'$. If $p\mid f$, there are at most $p+1$ such orbits.

This then implies:

$$\sum_{\substack{f\in V^i(\mathbb{Z})\\ p\nmid f\\ \text{but } GL_2(\mathbb{Z})f=GL_2(\mathbb{Z})\begin{pmatrix}p&0\\0&1\end{pmatrix}f'\\ \text{for some } f'\in V(\mathbb{Z})}} \alpha_T(f) \le 3\sum_{f'\in V^i(\mathbb{Z})} \alpha_{T/p^2}(f') + (p+1)\sum_{\substack{f'\in V^i(\mathbb{Z})\\ p\mid f'}} \alpha_{T/p^2}(f') \ll \frac{T}{p^2}.$$

<u>Pf of claim</u>

We have $\begin{pmatrix}p&0\\0&1\end{pmatrix}f''\in V(\mathbb{Z})$ if and only if $f''([0:1])\equiv 0 \bmod p$.

~~Consider the map~~ $\cancel{GL_2(\mathbb{Z})\to\mathbb{P}^1(\mathbb{F}_p)}$

$\cancel{M\mapsto M^T[0:1] \bmod p}$

We have $\begin{pmatrix}p&0\\0&1\end{pmatrix}M^Tf'\in V(\mathbb{Z})$ if and only if $M^T[0:1]$ is a root of f' mod p. If $M^T[0:1]\equiv M'^T[0:1] \bmod p$, then $GL_2(\mathbb{Z})\begin{pmatrix}p&0\\0&1\end{pmatrix}M f' = GL_2(\mathbb{Z})\begin{pmatrix}p&0\\0&1\end{pmatrix}M'f'$ because $M'M^{-1}\equiv\begin{pmatrix}*&*\\0&*\end{pmatrix} \bmod p$ and therefore $\begin{pmatrix}p&0\\0&1\end{pmatrix}M'M^{-1}\begin{pmatrix}p&0\\0&1\end{pmatrix}^{-1}\in GL_2(\mathbb{Z})$.

Hence, the number of orbits A is the nr. of roots of f' in $\mathbb{P}^1_{\mathbb{F}_p}$, which is ≤ 3 if $p \nmid f$ and $p+1$ if $p \mid f$.

claim $\rightarrow \Box$

Thm 15.5.9 $\rightarrow \Box$

Thm 15.5.1 $\rightarrow \Box$

15.6. Outlook on higher degrees

Rmk Every degree n form $f \in K[X,Y]$ with $\mathrm{disc}(f) \neq 0$ gives rise to an étale deg. n ext. of K (namely the ring of global sections of the vanishing locus of f on $\mathbb{P}^1_K$).

Every étale deg. n ext. arises from some f.

But for $n \geq 4$ there are "way more" $GL_2(K)$-orbits of forms than étale extensions: say K is algebraically closed.

$\dim(GL_2(K)) = 4$

$\dim(\{\text{deg. } n \text{ forms}\}) = n+1$

$\Rightarrow$ There are ∞ many orbits.

But there is only 1 étale ext.

Rmk $GL_2(\mathbb{Q}) \backslash \{\text{quartic forms with disc} \neq 0\} \leftrightarrow$ 2-Selmer elements of ell. curves

locally soluble

Thm (Wright–Yukie)

étale deg. 4 ext. $\longleftrightarrow (GL_2 \times GL_3)(K) \backslash \{(A,B)$ pair of ternary quadr. forms (with coeff. in K) $\mid \cdots \neq 0\}$

Thm (W–Y)

étale deg. 5 ext. $\Leftrightarrow (GL_4 \times GL_5)(K) \backslash \{(A_1,\dots,A_4)$ tuple of skew-symm. 5×5-matrices $\mid \cdots \neq 0\}$

Bhargava counted deg. 4,5 ext. of $\mathbb{Q}$ by discriminant by studying the relationship between rings of integers and integral orbits.

16. Abelian extensions

Let G be a finite abelian group.

Rmk 16.1

If $L|K$ is a Galois ext. with group G, we have a surjection $\Gamma_K \twoheadrightarrow \mathrm{Gal}(L|K) \xrightarrow{\sim} G$.

$\sigma \longmapsto \sigma|_L$

Conversely, any continuous surj. $f: \Gamma_K \twoheadrightarrow G$ arises from a Galois ext. with group G (the subfield of K^{sep} fixed by $\ker(f)$).

We'll count arbitrary cont. grp. hom. $\Gamma_K \twoheadrightarrow G$ (corr. to étale ext. vs. just field ext.)

~~If G is abelian, any hom.~~

Let K^{ab} be the maximal abelian ext. of K
(= compositum of all abelian ext.)
(= subext. of K^{sep} fixed by commutator subgr. of Γ_K)

For abelian G, any cont. hom. $\Gamma_K \to G$ factors through $\Gamma_K^{ab} = \mathrm{Gal}(K^{ab}|K)$.
Let K be a number field from now on.
For any p, let $I_p \subseteq \Gamma_K^{ab}$ be the inertia subgroup for p
(It's generally defined only up to conjugation!)

Def $f: \Gamma_K^{ab} \to G$ is unramified at p if $f(I_p) = \{id\}$.

Rmk 16.2 a) $L|K$ unram. at $p \iff$ corr. $f: \Gamma_K^{ab} \to G$ unram. at p.

b) Any f has only finitely many ramified primes p.