Math 295X Problem Set 4

Ashvin A. Swaminathan
swaminathan@math.harvard.edu

February 17, 2024

Problem 1

Let $f \in V(\mathbb{Z})$ be an integral binary cubic form, and let p be a prime such that $f \not\equiv 0 \pmod{p}$. Suppose that f factorizes modulo p as

$$f(x,y) \equiv \alpha \times \prod_i f_i^{e_i},$$

where $\alpha \in \mathbb{F}_p^\times$ and the f_i are distinct and irreducible binary forms of degree at most 3. Prove that we have the product decomposition

$$R_f/pR_f \simeq \prod_i \mathbb{F}_{p^{\deg f_i}}[t]/(t^{e_i}).$$

Hint: When $p \neq 2$, use the action of $\mathrm{GL}_2(\mathbb{F}_p)$ to ensure that none of the f_i are equal to y. This is not always possible when $p = 2$, but handle this case separately.

Problem 2

Let p be a prime. Determine the probability that $f \in V(\mathbb{Z})$ has each possible splitting type modulo p, and prove that the probability that R_f is maximal is $(1 - p^{-2})(1 - p^{-3})$.

Hint: Recall that R_f is automatically maximal if f has unramified splitting type; on the other hand, if f has ramified splitting type, then Dedekind's criterion gives a condition modulo p^2 for R_f to be maximal.

Problem 3

State a version of Davenport's Lemma for lattice points belonging to a residue class modulo m (in particular, determine how the error term depends on the modulus m). Use this version of the lemma to improve the error term in our asymptotic count of maximal cubic rings from $o(X)$ to $O(X^{5/6})$.