Enumerative arithmetic

Pagano, C.

Summary

Summary

This thesis consists of three chapters. Each chapter is on a different subject. However, all chapters address issues that arise in counting arithmetically interesting objects.

Chapter 1 is a joint paper with Peter Koymans about unit equations in positive characteristic. In this paper we establish the first upper bound that is uniform in the characteristic for the number of "solutions" to the unit equation. With this tool we settle a conjecture of F. Voloch. If p is a prime number, r a positive integer, K is a field with $\mathrm{char}(K) = p$ and $\Gamma \subseteq K^* \times K^*$ a finitely generated subgroup of rank r, the unit equation is the equation

$$x + y = 1,$$

to be solved in $(x, y) \in \Gamma$ but $(x, y) \notin \Gamma^p$. Denote by $S(\Gamma)$ the set of solutions to the unit equation for Γ. Our main theorem establishes that

$$\#S(\Gamma) \leq 31 \cdot 19^r.$$

Chapter 2 is a joint paper with Efthymios Sofos about statistical properties of ray class groups of fixed integral conductor of imaginary quadratic number fields. If c is a positive integer and K is a finite extension of $\mathbb{Q}$, the *ray class group* of conductor c of K is the group

$$\mathrm{Cl}(K, c) := \frac{I(K, c)}{\mathrm{Pr}(K, c)},$$

where $I(K, c)$ is the subgroup of $I_K := \{\text{fractional ideals in } K\}$ that is generated by ideals of O_K that are coprime to c and $\mathrm{Pr}(K, c)$ is the subgroup of I_K that is generated by principal ideals (α) with $\alpha \in O_K - \{0\}$ and α congruent to 1 modulo c. When K varies among imaginary quadratic number fields whose discriminant is coprime to c and congruent to 1 modulo 4, we establish the asymptotic behavior of the natural map

$$(2\mathrm{Cl}(K, c))[2] \to (2\mathrm{Cl}(K))[2],$$

obtaining as a corollary the joint distribution of

$$(\#2(\mathrm{Cl}(K, c))[2], \#(2\mathrm{Cl}(K))[2]).$$

Even though there is a surjective natural map $2\mathrm{Cl}(K, c) \twoheadrightarrow 2\mathrm{Cl}(K)$, the surjectivity of the induced map $(2\mathrm{Cl}(K, c))[2] \to (2\mathrm{Cl}(K))[2]$ encounters a cohomological obstruction. In a refined version of our main theorem, we show the equidistribution of this obstruction in the full obstruction group (viewed as a probability space with the counting measure).

These results extend the only previously known case, which is $c = 1$, where there is only the ordinary class group. This was due E. Fouvry and J. Klüners.

Next, we extend the Cohen–Lenstra and the Gerth heuristics from class groups to general ray class groups. The Cohen–Lenstra heuristic is a probabilistic model designed by H. Cohen and H. Lenstra, which predicts conjecturally the exact asymptotic outcome of most statistical questions about the $\mathbb{Z}[\frac{1}{2}]$-module $\mathrm{Cl}(K) \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{2}]$ as K varies among imaginary quadratic number fields. Later F. Gerth formulated a heuristic about $\mathrm{Cl}(K)[2^\infty]$. We formulate a more general probabilistic model aimed at predicting the exact asymptotic outcome of most statistical questions about ray class groups, viewed as exact sequences of Galois modules. This statistical model agrees with our result on 4-ranks, yielding a heuristic interpretation of the equidistribution of the above mentioned cohomological obstructions. Moreover, our model explains the precise constants given by a theorem of I. Varma about the average 3-torsion of ray class groups. With this statistical model for ray class groups, both our results on 4-ranks and Varma's result on the 3-torsion obtain a precise heuristical explanation and are placed within a broad conjectural framework.

Chapter 3 is about the arithmetic of local fields and it mostly focuses on the sub-class of p-adic fields for some prime number p. If p is a prime number, a p-adic field is a finite field extension $K/\mathbb{Q}_p$. The multiplicative group K^* carries a natural filtration

$$K^* \supseteq O_K^* \supseteq 1 + m_K \supseteq ... \supseteq 1 + m_K^i \supseteq ...,$$

where O_K denotes the ring of integers of K and m_K is its unique maximal ideal. One can show that the sequence

$$1 + m_K \supseteq ... \supseteq 1 + m_K^i \supseteq ...$$

is a filtration of $\mathbb{Z}_p$-modules. In this work I give a parametrization of the set of sequences of $\mathbb{Z}_p$-modules

$$M_1 \supseteq ... \supseteq M_i \supseteq ...$$

that are *isomorphic* to $1 + m_K \supseteq ... \supseteq 1 + m_K^i \supseteq ...$ for some local field K. This means that there exists an isomorphism of $\mathbb{Z}_p$-modules

$$\varphi : 1 + m_K \to M_1$$

such that $\varphi(1 + m_K^i) = M_i$. In case such a K exists, we say that the sequence $M_1 \supseteq ... \supseteq M_i \supseteq ...$ is *admissible*. I parametrize admissible sequences in terms of certain combinatorial objects called *jump sets*. One of the main theorems in this study is the remarkable property that this parametrization is *weight preserving*, in the following sense. It turns out that there is a natural way to attach to each jump set a weight. One can give the weight of a jump set also a natural interpretation in terms of the Haar measure. On the other hand, Serre introduced a natural probability measure on the set of totally ramified extensions of given degree of a given local field. In this chapter I show that the total mass of the set of local fields whose filtration of subgroups is isomorphic to a given admissible sequence equals the combinatorial weight of the corresponding jump set. Finally I use my identification between the set of jump sets and the set of admissible sequences to give a simpler and more conceptual proof of a classification, due to H. Miki, of the possible sets of *upper jumps* of a cyclic totally ramified p-power degree extension of a fixed p-adic field K.