Advances in Mathematics 258 (2014) 13–45

Contents lists available at ScienceDirect

Advances in Mathematics

www.elsevier.com/locate/aim

p^ℓ-torsion points in finite abelian groups and combinatorial identities

Christophe Delaunay [a], Frédéric Jouhet [b,*]

[a] Université de Franche-Comté, Laboratoire de Mathématiques de Besançon, CNRS UMR 6623, Facultés des Sciences et Techniques, 16 route de Gray, 25030 Besançon, France
[b] Université Claude Bernard Lyon 1, Institut Camille Jordan, CNRS UMR 5208, 43, boulevard du 11 novembre 1918, F-69622 Villeurbanne Cedex, France

A R T I C L E   I N F O

Article history:
Received 10 September 2012
Accepted 21 February 2014
Available online 26 March 2014
Communicated by Ravi Vakil

MSC:
11G05
11R29
11B75
20K01

Keywords:
Class groups of number fields
Tate–Shafarevich groups of elliptic curves
Heuristics
Symmetric functions
q-series

A B S T R A C T

The main aim of this article is to compute all the moments of the number of p^ℓ-torsion elements in some type of finite abelian groups. The averages involved in these moments are those defined for the Cohen–Lenstra heuristics for class groups and their adaptation for Tate–Shafarevich groups. In particular, we prove that the heuristic model for Tate–Shafarevich groups is compatible with the recent conjecture of Poonen and Rains about the moments of the orders of p-Selmer groups of elliptic curves. For our purpose, we are led to define certain polynomials indexed by integer partitions and to study them in a combinatorial way. Moreover, from our probabilistic model, we derive combinatorial identities, some of which appearing to be new, the others being related to the theory of symmetric functions. In some sense, our method therefore gives for these identities a somehow natural algebraic context.

* Corresponding author.
E-mail addresses: christophe.delaunay@univ-fcomte.fr (C. Delaunay), jouhet@math.univ-lyon1.fr (F. Jouhet).

http://dx.doi.org/10.1016/j.aim.2014.02.033

1. Introduction

In this work, we compute the averages, in some sense, of a large class of functions defined over some families of finite abelian groups. Theses averages come from the well-known Cohen–Lenstra heuristic model for understanding the behavior of class groups of number fields and their adaptation for Tate–Shafarevich[1] groups of elliptic curves (see [7,8,10,11]). In particular, our computations lead to a conjectural formula for all the moments of the number of n-torsion points in Tate–Shafarevich groups. We prove that our prediction is consistent with the recent model of Poonen and Rains that led them to conjecture a formula for all the moments of the number of n-torsion points in the Selmer groups of elliptic curves if n is squarefree (see [32]). Furthermore, our approach allows us to conjecture a formula for the moments of the number of n-torsion points in the Selmer groups of elliptic curves for all positive integers n (not only squarefree).

The computation of our averages involves several combinatorial tools. We introduce multivariate polynomials R_λ, indexed by integer partitions λ, depending on a fixed complex parameter t and we investigate combinatorial properties satisfied by them. As λ runs through all the set of integer partitions with parts bounded by a fixed integer ℓ, our polynomials form a basis of the polynomial ring $\mathbb{Z}(t)[x_1, x_2, \dots, x_\ell]$. Hence, these polynomials R_λ can be uniquely and explicitly expanded in terms of the monomials, thus defining an infinite ℓ-dimensional matrix, which can be explicitly inverted. The coefficients appearing in this inversion yield nice combinatorial expressions for our averages. Moreover, these coefficients appear to be related to a well-known algebraic combinatorial context, e.g., the problem of counting the number of subgroups of a finite abelian p-group with a given structure. This problem is actually at the heart of the construction of the Hall algebra, and the Hall–Littlewood symmetric polynomials. Furthermore, from the probabilistic model and the averages we computed, we obtain combinatorial identities involving q-series and the theory of Hall–Littlewood functions. A precise combinatorial analysis of the previously mentioned coefficients appearing in the inversion process allows us to prove that the Poonen and Rains model and the heuristic model for Tate–Shafarevich groups are compatible.

This article is organized as follows: in the next section, we recall the definitions of averages we consider. In Section 3, we fix some combinatorial notations and recall basic facts about integer partitions; we will also study some combinatorial identities related to the theory of Hall–Littlewood symmetric functions. Then, we define in Section 4 the polynomials R_λ and prove the above mentioned inversion formula. We also give some properties satisfied by the coefficients appearing in the inversion process, and we show how they are related to the problem of counting subgroups of finite abelian p-groups. In Section 5, we highlight the links between R_λ and finite abelian p-groups and deduce some averages. In Section 6, we briefly recall the philosophy of the heuristics on class

[1] Note that the original heuristic assumption for Tate–Shafarevich groups in [10] must be modified a little bit; this correction is explained in Section 6.2.