p^ℓ-TORSION POINTS IN FINITE ABELIAN GROUPS AND COMBINATORIAL IDENTITIES

CHRISTOPHE DELAUNAY AND FRÉDÉRIC JOUHET

ABSTRACT. 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.

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 heuristics model for understanding the behavior of class groups of number fields and their adaptation for Tate-Shafarevich[1] groups of elliptic curves (see [CL84, CM90, Del01, Del07]). 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 [PR12]). 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 integer 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 $\mathbb{Z}(t)[x_1, x_2, \ldots, x_\ell]$. 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 groups and on Tate-Shafarevich groups and give several consequences of our formulas on heuristics. In particular, concerning the Tate-Shafarevich groups of elliptic curves, we discuss how the heuristics principle and the Poonen and Rains model complement each other. Finally, we end the paper in Section 7 by some combinatorial consequences and related questions.

2. u-AVERAGES ON FINITE ABELIAN p-GROUPS AND MOTIVATIONS

Throughout the paper, p will always denote a prime number. The letter H (or H_λ if H is indexed by an integer partition λ) is used for an isomorphism class of a finite abelian p-group and the letter G (or G_λ) is used for an isomorphism class of a (finite abelian) p-group of type S. As in [Del01, Del07], we say that a p-group G is of type S if G is a finite abelian p-group endowed with a non-degenerate, bilinear, alternating pairing:

$$\beta \ : \ G \times G \to \mathbb{Q}/\mathbb{Z}.$$

An isomorphism of groups of type S is an isomorphism of groups preserving the pairings. A p-group of type S has the form $G = H \times H$. Reciprocally, each group G, of the form $H \times H$ has a unique structure of group of type S up to isomorphism. In particular, if G is a group of type S then $|\operatorname{Aut}^s(G)|$, the number of automorphisms of G that respect the (underlying) pairing β, does not depend on β. Due to these facts, the pairings associated to groups of type S will never be specified in the sequel.

2.1. **Definitions of u-averages.** Let h be a complex-valued function defined on isomorphism classes of finite abelian p-groups and let u be a nonnegative real number. In [CL84], Cohen and Lenstra defined an u-average[2] $\mathrm{M}_u(h)$, of the function h (in particular, if h is the characteristic function of a property $\mathcal{P}$, $\mathrm{M}_u(h)$ is called the u-probability of $\mathcal{P}$), and we have

$$\mathrm{M}_u(h) = \frac{\displaystyle\sum_{n \geqslant 1} p^{-nu} \sum_{H(p^n)} \frac{h(H)}{|\operatorname{Aut}(H)|}}{\displaystyle\prod_{j \geqslant 1} \left(1 - p^{-u-j}\right)^{-1}},$$

if the first sum on the numerator converges, and where $\sum_{H(p^n)}$ means that the sum is over all isomorphism classes of finite abelian groups H of order p^n. The number

---

[2]Actually, the u-averages $\mathrm{M}_u(h)$, as well as $\mathrm{M}_u^S(h)$, are defined for all finite abelian groups, not only for p-groups. However, for the functions h we have in mind, all the p-parts behave independently.

$\mathrm{M}_u(h)$ is indeed an average since whenever $h \equiv 1$ we have $\mathrm{M}_u(h) = 1$, i.e. (see [Hal38, CL84])

$$\prod_{j \geqslant 1} \left(1 - p^{-u-j}\right)^{-1} = \sum_{n \geqslant 1} p^{-nu} \sum_{H(p^n)} \frac{1}{|\operatorname{Aut}(H)|}.$$

Cohen and Lenstra introduced such averages as a heuristic model in order to give precise predictions for the behavior of class groups of number fields varying in certain natural families. We will come back to this notion and give some examples later.

The aim of [Del01] was to adapt Cohen-Lenstra's model, to give predictions for the behavior of Tate-Shafarevich groups of elliptic curves varying in certain natural families. Recall that if they are finite (as it is classically conjectured), Tate-Shafarevich groups are groups of type S. One can define, for a nonnegative real number u, the u-average (in the sense of groups of type S), denoted by $\mathrm{M}_u^s(g)$, for a function g defined on isomorphism classes of groups of type S. We have

$$\mathrm{M}_u^s(g) = \frac{\displaystyle\sum_{n \geqslant 1} p^{-nu} \sum_{G(p^n)} \frac{|G|\, g(G)}{|\operatorname{Aut}^s(G)|}}{\displaystyle\prod_{j \geqslant 1} \left(1 - p^{-2u-2j+1}\right)^{-1}},$$

if the first sum on the numerator converges, and where $\sum_{G(p^n)}$ means that the sum is over all isomorphism classes of groups G of type S and order p^n (the sum being empty if n is odd). As above, the number $\mathrm{M}_u^s(g)$ is an average since if $g \equiv 1$, then $\mathrm{M}_u^s(g) = 1$, i.e. (see [Del01]),

$$\prod_{j \geqslant 1} \left(1 - p^{-2u-2j+1}\right)^{-1} = \sum_{n \geqslant 1} p^{-nu} \sum_{G(p^n)} \frac{|G|}{|\operatorname{Aut}^s(G)|} = \sum_{n \geqslant 1} p^{-2nu} \sum_{G(p^{2n})} \frac{|G|}{|\operatorname{Aut}^s(G)|}.$$

As for finite abelian groups, $\mathrm{M}_u^s(g)$ will be called the u-probability of $\mathcal{P}$ if g is the characteristic function of a property $\mathcal{P}$ for groups of type S. It will always be clear in the context whether we are concerned with averages in the sense of finite abelian groups or groups of type S.

If h is defined over isomorphism classes of finite abelian p-groups, it is not difficult to deduce the u-average $\mathrm{M}_u^s(h)$ of h restricted to isomorphism classes of p-groups ot type S from $\mathrm{M}_u(h)$, the u-average of h in the sense of finite abelian groups (see [Del07, Del11]), and reciprocally.

2.2. **Motivations.** The goal of [Del11] was to study the probability laws of the p^ℓ-ranks of abelian p-groups (resp. p-groups of type S) in the sense of the above probability model. In particular, a closed formula was given for the u-averages of the function $h(H) = |H[p^\ell]|$ (resp. $g(G) = |G[p^\ell]|$) for any integer $\ell \geqslant 0$, where $H[p^\ell]$ denotes the p^ℓ-torsion elements subgroup of H. Such computations were motivated by a question of M. Bhargava about the heuristics for Tate-Shafarevich groups and their comparison with theoretical results of Bhargava and Shankar ([BS10b, BS10a]) about the distribution of p-Selmer groups (with $p = 2$ and 3) of all elliptic curves.

From this point of view, our work aims to generalize the study in [Del11], and to give formulas for the u-averages of $h(H) = |H[p^\ell]|^{m_\ell}$ (resp. $g(G) = |G[p^\ell]|^{m_\ell}$) for all integers $\ell \geqslant 0$ and $m_\ell \geqslant 0$. As we will see later, the computations are much more technical as they involve deeper combinatorial tools. Roughly speaking, in order to evaluate the u-average of $h(H) = |H[p^\ell]|^{m_\ell}$, we will more generally compute the u-averages of any function $h(H) = |H[p]|^{m_1}|H[p^2]|^{m_2} \cdots |H[p^\ell]|^{m_\ell}$ for all nonnegative integers $m_1, m_2, \ldots, m_\ell$. We are able to find a formula by induction; but actually we directly obtain a closed formula by using a ℓ-dimensional matrix

inversion result which takes the place of the recursion principle. The motivation for this computation will be explained in the next section and comes originally from the following question of Poonen: take $g(G) = |G[p^\ell]|^{m_\ell}$; is it true that $\mathrm{M}_0^s(g) = \mathrm{M}_1^s(g) \cdot p^{\ell m_\ell}$? We will actually positively answer this question, by proving the following more general result.

Theorem 1. *For any positive integer ℓ, let $m_1, m_2, \ldots, m_\ell$ be ℓ nonnegative integers. Consider the following function g defined on isomorphism classes of p-groups of type S:*

$$g(G) = |G[p]|^{m_1} |G[p^2]|^{m_2} \cdots |G[p^\ell]|^{m_\ell}.$$

Then we have

$$\mathrm{M}_0^s(g) = \mathrm{M}_1^s(g)\, p^{m_1 + 2m_2 + \cdots + \ell m_\ell}.$$

As we will explain, the fact that the answer to Poonen's question is indeed positive makes the Poonen-Rains model for Selmer groups compatible with the heuristics for Tate-Shafarevich groups.

From a combinatorial point of view, our computations and the tools they require (including the probabilistic model for abelian p-groups), allow us to obtain a family of interesting combinatorial identities. Some of them are related to summation formulas for Hall-Littlewood symmetric functions, and can be proved in a non trivial way through this theory, while others seem to be new, or at least not direct consequences of previous known identities of the same type. At the heart of our computations appears some coefficients, denoted by $C_{\lambda,\mu}(q)$ (where λ and μ are integer partitions), which satisfy nice combinatorial properties, and, setting $q = 1/p$, are related to the number of subgroups H_μ in a finite abelian p-group H_λ (a group H_λ is often called a *group of type λ*[3]). In particular, their symmetry relation given by Theorem 5 yields a proof of Theorem 1, and therefore a positive answer to Poonen's question. As we will see, Theorem 5 is actually a consequence of a well-known property in the framework of finite abelian p-groups [But94, Del48], and therefore related to Hall-Littlewood symmetric polynomials. We shall however give an alternative proof of this symmetry property by using a general summation formula (due to Lascoux [Las07]) of Hall-Littlewood functions. Finally, to prove Theorem 1, we will also need an evaluation of the number of injective homomorphisms of a group H_λ into the finite abelian p-group H, associated to a result of Cohen and Lenstra from [CL84].

3. Integer partitions and Hall-Littlewood functions

3.1. **Notations and definitions.** Recall that a *partition* $\lambda := (\lambda_1 \geqslant \lambda_2 \geqslant \cdots)$ of a nonnegative integer n is a finite decreasing sequence of nonnegative integers whose sum is equal to n. We often use the notation $|\lambda| := \sum_{i=1}^{\ell} \lambda_i = n$, and the integer $\ell = \ell(\lambda) = max\{i | \lambda_i > 0\}$ is called the *length* of the integer partition λ. We will also denote by $\lambda \vdash n$ the fact that λ is a partition of the integer n. The integers λ_i (for $1 \leqslant i \leqslant \ell$) are the *parts* of λ. It is also convenient to write an integer partition by its *multiplicities*: we denote by $m_i = m_i(\lambda) := \#\{j | \lambda_j = i\} \geqslant 0$ the multiplicity of the integer i in λ. Therefore the partition λ can be written $\lambda = 1^{m_1} 2^{m_2} \ldots$, and we have $n = m_1 + 2m_2 + \cdots$. Finally, we denote by λ' the *conjugate* partition of λ, whose parts are $\lambda_i' := \#\{j | \lambda_j \geqslant i\}$, for $1 \leqslant i \leqslant \lambda_1$. Thus we have $|\lambda'| = |\lambda|$, $\ell(\lambda') = \lambda_1$, and for any integer i, $m_i(\lambda) = \lambda_i' - \lambda_{i+1}'$ (and

---

[3]If $\lambda := (\lambda_1 \geqslant \lambda_2 \cdots)$ is a partition, a p-group H_λ is said to be a group of type λ if it is isomorphic to $\mathbb{Z}/p^{\lambda_1}\mathbb{Z} \oplus \mathbb{Z}/p^{\lambda_2}\mathbb{Z} \oplus \cdots$. We will not use this terminology in order to avoid any confusion with the notion of group of type S we introduced before.

equivalently $m_i(\lambda') = \lambda_i - \lambda_{i+1}$).

We will also use the following standard statistic on integer partitions

$$n(\lambda) := \sum_{i \geqslant 1}(i-1)\lambda_i = \sum_{i \geqslant 1}\binom{\lambda_i'}{2}.$$

Next we recall some standard definitions and notations for q-series, which can be found in [GR04]. Let q be a fixed complex parameter (the "base") with $|q| \neq 1$. We define for any real number a and any $k \in \mathbb{Z}$ the *q-shifted factorial* by

$$(a)_k \equiv (a;q)_k := \begin{cases} 1 \text{ if } k = 0 \\ (1-a)\dots(1-aq^{k-1}) \text{ if } k > 0 \\ 1/(1-aq^{-1})\dots(1-aq^k) \text{ if } k < 0, \end{cases}$$

and $(a)_\infty := \lim_{k \to +\infty}(a)_k$. The base q can be omitted when there is no confusion (writing $(a)_k$ for $(a;q)_k$, etc). For the sake of simplicity, write for $k \in \mathbb{Z} \cup \{\infty\}$

$$(a_1,\dots,a_m)_k := (a_1)_k \times \dots \times (a_m)_k.$$

Recall also the definition of the *q-binomial coefficient*

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \frac{(q)_n}{(q)_k(q)_{n-k}},$$

which is a polynomial in the variable q, with positive integral coefficients.

We will need later a special case of the so-called finite q-binomial theorem (see for instance [GR04]), which for any complex number z and any nonnegative integer n, can be written as follows

$$(1) \qquad \sum_{k=0}^{n}(-1)^k z^k q^{k(k-1)/2}\begin{bmatrix} n \\ k \end{bmatrix}_q = (z)_n.$$

Next, we recall some basic facts about the theory of Hall-Littlewood functions, which can be found with more details in [Mac95, Chapter III]. Hall-Littlewood polynomials were introduced by Hall to evaluate the number of subgroups of type μ and cotype ν in a finite abelian p-group of type λ, and expressed explicitly later by Littlewood (see for instance [But94] for detailed explanations of this construction). Let S_n be the symmetric group, $\Lambda_n = \mathbb{Z}[x_1,\dots,x_n]^{S_n}$ be the ring of symmetric polynomials in n independant variables and Λ be the ring of symmetric functions in countably many independant variables. For a set of n variables $x = \{x_1,\dots,x_n\}$, the Hall-Littlewood polynomials $P_\lambda(x;q)$ are defined by

$$P_\lambda(x;q) := \prod_{i \geqslant 1}\frac{(1-q)^{m_i}}{(q)_{m_i}}\sum_{w \in S_n}w\left(x_1^{\lambda_1}\dots x_n^{\lambda_n}\prod_{i<j}\frac{x_i - qx_j}{x_i - x_j}\right),$$

where w acts by permuting the variables. These polynomials are symmetric in x, homogeneous of degree $|\lambda|$, with coefficients in $\mathbb{Z}[q]$, and form a $\mathbb{Z}[q]$ basis of $\Lambda_n[q]$, which interpolates between monomial (for $q = 1$) and Schur (for $q = 0$) polynomials. Moreover, thanks to their classical stability property, they may be extended to the Hall-Littlewood functions in an infinite number of variables in order to form a $\mathbb{Z}[q]$ basis of $\Lambda[q]$. Another useful result is the specialization

$$(2) \qquad P_\lambda(z, zq, \dots, zq^{n-1}; q) = \frac{z^{|\lambda|}q^{n(\lambda)}(q)_n}{(q)_{n-\ell(\lambda)}b_\lambda(q)},$$

where

$$b_\lambda(q) := \prod_{i \geqslant 1}(q)_{\lambda_i' - \lambda_{i+1}'}.$$

Finally, by using the Cauchy identity for Hall-Littlewood polynomials [Mac95, p. 224, (4.4)], the specialization (2), and the Pieri formula [Mac95, p. 224, (3.2)], it is possible to derive the following identity from [Mac95], which can be seen as a q-binomial theorem for Hall-Littlewood functions

$$(3) \qquad \sum_\lambda q^{n(\lambda)}(a;q^{-1})_{\ell(\lambda)}P_\lambda(x;q) = \prod_{i\geqslant 1}\frac{1-ax_i}{1-x_i},$$

where a is a complex number, and the summation is taken over all integer partitions.

3.2. Lascoux's summation of Hall-Littlewood functions.

The Rogers-Ramanujan identities are two of the most famous q-series identities, with deep connections to many branches of mathematics. Lots of proofs of these identities have been given, among which one by Stembridge in [Ste90], who generalized work by Macdonald from [Mac95] to show that the Rogers-Ramanujan identities (among others) may be obtained by appropriate specializations of finite summations for Hall-Littlewood polynomials. In [ASW99], Andrews, Schilling and Warnaar generalized the Rogers-Ramanujan identities to three identities labelled by the Lie algebra A_2. Later, seeking a way of proving the latter through the theory of Hall-Littlewood polynomials as Stembridge did for the Rogers-Ramanujan identities, Warnaar showed in [War06] the following A_2-type identity for Hall-Littlewood functions

$$(4) \quad \sum_{\lambda,\,\mu} q^{n(\lambda)+n(\mu)-(\lambda'|\mu')}P_\lambda(x;q)P_\mu(y;q) = \prod_{i\geqslant 1}\frac{1}{(1-x_i)(1-y_i)}\prod_{i,j\geqslant 1}\frac{1-x_iy_j}{1-x_iy_j/q},$$

where the sum is over all pairs of integers partitions, and $(\lambda|\mu) := \sum_{i\geqslant 1}\lambda_i\mu_i$. In [War06], Warnaar explains how (4) yields one of the three A_2-type Rogers-Ramanujan identities from [ASW99].

For our purpose, we will actually need a generalization of (4), which was discovered and proved by Lascoux in [Las07]. To this aim, he used the modified Hall-Littlewood polynomials Q'_μ, which form the adjoint basis of P_λ with respect to the Hall scalar product (see [Las07, Mac95] for details). More precisely, Lascoux's formula can be written as

$$(5) \qquad \sum_\lambda\sum_{\mu\subseteq\lambda} P_\lambda(x;q)P_\mu(y;q)b_\lambda(q)Q'_{\lambda/\mu}(\mathbf{1};q) = \prod_{i\geqslant 1}\frac{1}{1-x_i}\prod_{j\geqslant 1}\frac{1-qx_iy_j}{1-x_iy_j},$$

where $\mu\subseteq\lambda$ means that $\mu_i\leqslant\lambda_i$ for all integers i, $Q'_{\lambda/\mu}$ are the skew modified Hall-Littlewood polynomials, and the coefficients $Q'_{\lambda/\mu}(\mathbf{1};q)$ are explicitely given by

$$(6) \qquad Q'_{\lambda/\mu}(\mathbf{1};q) = q^{|\mu|+n(\lambda)+n(\mu)-(\lambda'|\mu')}\prod_{i\geqslant 1}\begin{bmatrix}\lambda'_i-\mu'_{i+1}\\\lambda'_i-\mu'_i\end{bmatrix}_q.$$

It is easy to see that $Q'_{\lambda/\mu}(\mathbf{1};q)$ are polynomials in the variable q, with positive integral coefficients, for which Lascoux gave a combinatorial interpretation in [Las07]. As remarked in [WZ12], setting $q=1/p$ with p a prime number, $Q'_{\lambda/\mu}(\mathbf{1};1/p)$ are related to the number of subgroups of type μ in a finite abelian p-group of type λ. We will come back to this link in the next section. Finally, although it is not trivial at first sight, Lascoux showed in [Las07] how Warnaar's identity (4) is a consequence of (5).

4. THE POLYNOMIALS $R_\lambda(x,t)$

For our purpose, we fix a positive integer ℓ, and we consider a partition $\lambda = (\lambda_1\geqslant\lambda_2\geqslant\cdots)$ such that $\lambda_1\leqslant\ell$ (i.e., the length of the conjugate partition λ'

satisfies $\ell(\lambda') \leqslant \ell$). For a set of ℓ variables $x = \{x_1, \ldots, x_\ell\}$ (adding the convention $x_0 := 1$) and a complex parameter t, we define the polynomial[4]

$$(7) \qquad R_\lambda(x; t) := \prod_{i=1}^{\ell} \prod_{j=\lambda'_{i+1}}^{\lambda'_i - 1} (x_i - t^j x_{i-1}),$$

which can be rewritten through the multiplicities $m_1, \ldots, m_\ell$ of the partition λ as follows

$$R_\lambda(x; t) = \prod_{i=1}^{\ell} x_i^{\lambda'_i - \lambda'_{i+1}} \prod_{j=0}^{\lambda'_i - \lambda'_{i+1} - 1} \left(1 - t^{j + \lambda'_{i+1}} \frac{x_{i-1}}{x_i}\right)$$

$$(8) \qquad = \prod_{i=1}^{\ell} x_i^{m_i} (t^{m_{i+1} + \cdots + m_\ell} x_{i-1}/x_i; t)_{m_i}.$$

It is clear that whenever λ runs through all partitions with $\lambda_1 \leqslant \ell$, then the polynomials $R_\lambda(x; t)$ form a basis of $\mathbb{Z}(t)[x_1, x_2, \ldots, x_\ell]$.

Our goal is to expand the polynomial R_λ in terms of the monomials $x_1^{k_1} \ldots x_\ell^{k_\ell}$, and to invert this relation. To this aim, writing $\lambda = 1^{m_1} 2^{m_2} \ldots$, we have to express the monomial $x_1^{m_1} \ldots x_\ell^{m_\ell}$ in terms of the polynomials $R_\mu(x; t)$, where $\mu = (\mu_1 \geqslant \mu_2 \geqslant \ldots)$ are integer partitions included in λ, i.e., satisfying $\mu_i \leqslant \lambda_i$ for any integer i (note that this is equivalent to the conditions $\mu'_i \leqslant \lambda'_i$ for any integer i).

It is easy to see that R_λ can be expanded as a sum of monomials x^μ for $\mu \subseteq \lambda$, and this is what we explicitly do in the next proposition.

Proposition 2. *We have*

$$R_\lambda(x; q) = \sum_{\mu \subseteq \lambda} x_1^{\mu'_1 - \mu'_2} \ldots x_\ell^{\mu'_\ell} (-1)^{|\lambda| - |\mu|} q^{n(\lambda \backslash \mu)}$$

$$\times q^{\lambda'_2(\lambda'_1 - \mu'_1) + \cdots + \lambda'_\ell(\lambda'_{\ell-1} - \mu'_{\ell-1})} \prod_{i \geqslant 1} \begin{bmatrix} \lambda'_i - \lambda'_{i+1} \\ \lambda'_i - \mu'_i \end{bmatrix}_q.$$

Proof. We expand the expression (8) of the polynomials $R_\lambda(x; q)$ by using ℓ times the q-binomial theorem (1), which yields

$$R_\lambda(x; q) = \sum_{k_1, \ldots, k_\ell} x_1^{m_1 - k_1 + k_2} \ldots x_{\ell-1}^{m_{\ell-1} - k_{\ell-1} + k_\ell} x_\ell^{m_\ell - k_\ell} (-1)^{k_1 + \cdots + k_\ell}$$

$$\times q^{\binom{k_1}{2} + \cdots + \binom{k_\ell}{2}} q^{(m_2 + \cdots + m_\ell)k_1 + \cdots + m_\ell k_{\ell-1}} \begin{bmatrix} m_1 \\ k_1 \end{bmatrix}_q \cdots \begin{bmatrix} m_\ell \\ k_\ell \end{bmatrix}_q.$$

Definig the integer partition μ by $\mu = 1^{k_1} 2^{k_2} \ldots \ell^{k_\ell}$, and replacing in this expression k_i by $\lambda'_i - \mu'_i$, we obtain the formula. $\qquad \square$

We are now interested in the reciprocal identity, i.e., the expansion of the monomials x^λ in terms of the polynomials R_μ. For this, we need the following multidimensional matrix inversion, which was communicated to us by Michael Schlosser.

Lemma 3. *The infinite lower-triangular ℓ-dimensional matrices $F = (F_{\boldsymbol{a},\boldsymbol{b}})_{\boldsymbol{a},\boldsymbol{b} \in \mathbb{Z}^\ell}$ and $G = (G_{\boldsymbol{a},\boldsymbol{b}})_{\boldsymbol{a},\boldsymbol{b} \in \mathbb{Z}^\ell}$ are inverses of each other, where*

$$F_{\boldsymbol{a},\boldsymbol{b}} = (-1)^{|\boldsymbol{a}| - |\boldsymbol{b}|} q^{\sum_{i=1}^{\ell} \left(\binom{a_i + 1}{2} + \binom{b_i}{2} + a_i b_{i+1}\right)} \prod_{i=1}^{\ell} \frac{(q)_{a_i - b_{i+1}}}{(q)_{a_i - b_i}},$$

---

[4]Note that we take the parameter t in order to avoid confusions since we will need to specialize $t = q$ and $t = 1/q$ later.

and

$$G_{\boldsymbol{a},\boldsymbol{b}} = q^{-\sum_{i=1}^{\ell} b_i(a_i+a_{i+1})} \prod_{i=1}^{\ell} \frac{1}{(q)_{a_i-b_i}(q)_{b_i-a_{i+1}}},$$

with $a_{\ell+1} = b_{\ell+1} = 0$ and $|\boldsymbol{a}| = a_1 + \cdots + a_\ell$, $|\boldsymbol{b}| = b_1 + \cdots + b_\ell$.

Proof. We will see that the previous inversion follows from a suitable specialization of a multidimensional matrix inversion due to Schlosser in [Sch07], which is itself a special case of the inversion of the Pieri rule for Macdonald polynomials [LS06, Theorem 2.6]. First recall that the infinite lower-triangular ℓ-dimensional matrices $F = (F_{\mathbf{a},\mathbf{b}})_{\mathbf{a},\mathbf{b}\in\mathbb{Z}^\ell}$ and $G = (G_{\mathbf{a},\mathbf{b}})_{\mathbf{a},\mathbf{b}\in\mathbb{Z}^\ell}$ are inverses of each other means that for any pair of infinite ℓ-dimensional vectors $\alpha_{\mathbf{a}}$ and $\beta_{\mathbf{b}}$, we have

(9) $$\alpha_{\mathbf{a}} = \sum_{\mathbf{b}\leqslant\mathbf{a}} F_{\mathbf{a},\mathbf{b}}\,\beta_{\mathbf{b}} \Leftrightarrow \beta_{\mathbf{a}} = \sum_{\mathbf{b}\leqslant\mathbf{a}} G_{\mathbf{a},\mathbf{b}}\,\alpha_{\mathbf{b}},$$

where $\mathbf{b} \leqslant \mathbf{a}$ means that $b_i \leqslant a_i$ for all integers $i \in \{1,\ldots,\ell\}$. Now in [Sch07, (A.9)], replace n by ℓ, let $t_0 \to 0$ and $t_i \mapsto u_i/u_{i+1}$ for $i = 1,\ldots,\ell$. We denote by $(f_{\mathbf{a},\mathbf{b}})_{\mathbf{a},\mathbf{b}\in\mathbb{Z}^\ell}$ and $(g_{\mathbf{a},\mathbf{b}})_{\mathbf{a},\mathbf{b}\in\mathbb{Z}^\ell}$ the resulting infinite lower-triangular ℓ-dimensional matrices, which are inverses of each other. Then we define infinite invertible diagonal ℓ-dimensional matrices D and E by

$$D_{\mathbf{a}} := u_1^{a_1} u_2^{2a_2-a_1} \ldots u_\ell^{\ell a_\ell-(\ell-1)a_{\ell-1}} u_{\ell+1}^{-\ell a_\ell} (-1)^{a_\ell} \prod_{i=1}^{\ell-1}(q)_{a_i-a_{i+1}}$$
$$\times q^{a_\ell^2/2+a_\ell/2-\sum_{i=1}^{\ell}(a_i a_{i+1}-ia_i)}$$

and

$$E_{\mathbf{b}} := u_1^{b_1} u_2^{2b_2-b_1} \ldots u_\ell^{\ell b_\ell-(\ell-1)b_{\ell-1}} u_{\ell+1}^{-\ell b_\ell} (-1)^{b_\ell} (q)_{b_\ell} \times q^{b_\ell^2/2+b_\ell/2-\sum_{i=1}^{\ell}(b_i^2-ib_i)}.$$

It is clear that through the definition in (9), the matrices $(D_{\mathbf{b}}f_{\mathbf{a},\mathbf{b}}E_{\mathbf{a}}^{-1})_{\mathbf{a},\mathbf{b}\in\mathbb{Z}^\ell}$ and $(E_{\mathbf{b}}g_{\mathbf{a},\mathbf{b}}D_{\mathbf{a}}^{-1})_{\mathbf{a},\mathbf{b}\in\mathbb{Z}^\ell}$ are still inverses of each other. Finally, we let $u_1 \to \infty$, then $u_2 \to \infty$, ... , $u_\ell \to \infty$ (in this order) in the previous matrices, which yields after some complicated but elementary manipulations

$$\lim_{u_1,\ldots,u_\ell\to\infty} D_{\mathbf{b}}f_{\mathbf{a},\mathbf{b}}E_{\mathbf{a}}^{-1} = F_{\mathbf{a},\mathbf{b}},$$

and

$$\lim_{u_1,\ldots,u_\ell\to\infty} E_{\mathbf{b}}g_{\mathbf{a},\mathbf{b}}D_{\mathbf{a}}^{-1} = G_{\mathbf{a},\mathbf{b}}.$$

This completes the proof. $\square$

Now we are able to prove the following result, which is our desired inversion.

Theorem 4. *For any positive integer ℓ, and an integer partition $\lambda = 1^{m_1}2^{m_2}\ldots\ell^{m_\ell}$, we have*

$$x_1^{m_1}\ldots x_\ell^{m_\ell} = \sum_{\mu\subseteq\lambda} C_{\lambda,\,\mu}(q)\,R_\mu(x;q),$$

where

(10) $$C_{\lambda,\,\mu}(q) := q^{\sum_{i=1}^{\ell}\mu'_{i+1}(\lambda'_i-\mu'_i)} \prod_{i\geqslant 1} \begin{bmatrix} \lambda'_i-\mu'_{i+1} \\ \lambda'_i-\mu'_i \end{bmatrix}_q.$$

Proof. Recall that we have

$$R_\lambda(x;q) = \sum_{\mu\subseteq\lambda} x_1^{\mu'_1-\mu'_2}\ldots x_\ell^{\mu'_\ell}(-1)^{|\lambda|-|\mu|}\,q^{\binom{\lambda'_1-\mu'_1}{2}+\cdots+\binom{\lambda'_\ell-\mu'_\ell}{2}}$$

$$\times q^{\lambda'_2(\lambda'_1-\mu'_1)+\cdots+\lambda'_\ell(\lambda'_{\ell-1}-\mu'_{\ell-1})} \begin{bmatrix} \lambda'_1-\lambda'_2 \\ \lambda'_1-\mu'_1 \end{bmatrix}_q \cdots \begin{bmatrix} \lambda'_\ell \\ \lambda'_\ell-\mu'_\ell \end{bmatrix}_q.$$

In order to use the inversion of Lemma 3, we observe that this relation is equivalent to the following:

$$(11) \qquad \beta_{\mathbf{a}} = \sum_{\mathbf{b} \leqslant \mathbf{a}} G_{\mathbf{a},\mathbf{b}} \, \alpha_{\mathbf{b}},$$

where $a_i = \lambda_i'$, $b_i = \mu_i'$,

$$\beta_{\mathbf{a}} := (-1)^{|\mathbf{a}|} \frac{q^{-\sum_{i=1}^{\ell}\left(\binom{a_i}{2}+a_i a_{i+1}\right)}}{(q)_{a_1-a_2}\cdots(q)_{a_l}} R_\lambda(x;q),$$

and

$$\alpha_{\mathbf{b}} := (-1)^{|\mathbf{b}|} q^{\sum_{i=1}^{\ell}\binom{b_i+1}{2}} x_1^{b_1-b_2}\ldots x_\ell^{b_\ell}.$$

The multidimensional matrix inversion in Lemma 1 applied to (11) yields

$$\alpha_{\mathbf{a}} = \sum_{\mathbf{b} \leqslant \mathbf{a}} F_{\mathbf{a},\mathbf{b}} \, \beta_{\mathbf{b}},$$

which is equivalent to

$$x_1^{a_1-a_2}\ldots x_\ell^{a_\ell} = \sum_{\mathbf{b}\leqslant\mathbf{a}} q^{\sum_{i=1}^{\ell} b_{i+1}(a_i-b_i)} \prod_{i=1}^{\ell} \frac{(q)_{a_i-b_{i+1}}}{(q)_{b_i-b_{i+1}}(q)_{a_i-b_i}} R_\mu(x;q),$$

and this completes the proof after replacing the variables a_i by λ_i' and b_i by μ_i', and then recalling the definition of the q-binomial coefficient. $\qquad\square$

Remark. It is easy to see from its definition that $C_{\lambda,\mu}(q)$ is a polynomial in the variable q, with positive integral coefficients. Moreover, thanks to the classical transformation $\begin{bmatrix} n \\ k \end{bmatrix}_{1/q} = q^{k(k-n)} \begin{bmatrix} n \\ k \end{bmatrix}_q$, it is related to the coefficient $Q'_{\lambda/\mu}\mathbf{1}$ (defined in (6)) by

$$(12) \qquad C_{\lambda,\mu}(1/q) = q^{n(\mu)-n(\lambda)} Q'_{\lambda/\mu}(\mathbf{1};q),$$

which, by setting $q = 1/p$ with p a prime number, counts exactly the number of subgroups of type μ in a finite abelian p-group of type λ (see [Del48, But94]).

Thanks to this remark, the following symmetry property satisfied by the coefficients $C_{\lambda,\mu}(q)$ becomes a direct consequence of the Pontryagin duality for finite abelian groups. However, we give below a very natural proof which uses Lascoux's formula (5), therefore highlighting and exploiting the link, given by (12), between these coefficients and Hall-Littlewood functions.

Theorem 5. *Let m and k be two nonnegative integers, and λ be a partition of m. Then we have*

$$\sum_{\substack{|\mu|=k \\ \mu\subseteq\lambda}} C_{\lambda,\mu}(q) = \sum_{\substack{|\mu|=m-k \\ \mu\subseteq\lambda}} C_{\lambda,\mu}(q).$$

Equivalently, the polynomial $\displaystyle\sum_{\mu\subseteq\lambda} C_{\lambda,\mu}(q)T^{|\mu|} \in \mathbb{N}[q][T]$ is self-reciprocal.

Proof. We will actually show the following equivalent form of the theorem

$$(13) \qquad \sum_{\substack{|\mu|=k \\ \mu\subseteq\lambda}} C_{\lambda,\mu}(1/q) = \sum_{\substack{|\mu|=m-k \\ \mu\subseteq\lambda}} C_{\lambda,\mu}(1/q).$$

In Lascoux's formula (5), consider the specialization $y = \{z, zq, zq^2, \ldots\}$, and use the $n \to \infty$ case of (2), together with (12) and the homogeneity of the Hall-Littlewood polynomials to derive

$$(14) \qquad \sum_\lambda \sum_{\mu \subseteq \lambda} q^{n(\lambda)} P_\lambda(x; q) z^{|\mu|} C_{\lambda,\mu}(1/q) = \prod_{i \geqslant 1} \frac{1}{(1-x_i)(1-zx_i)},$$

which is the generating function for the left-hand side of (13). We then compute the same generating function for the right-hand side of (13)

$$\sum_{k \geqslant 0} \sum_\lambda q^{n(\lambda)} P_\lambda(x; q) z^{|\lambda|-k} \sum_{\substack{|\mu|=|\lambda|-k \\ \mu \subseteq \lambda}} C_{\lambda,\mu}(1/q)$$

$$= \sum_{\lambda,\mu \,|\, \mu \subseteq \lambda} q^{n(\lambda)} P_\lambda(x; q) z^{|\lambda|-|\mu|} C_{\lambda,\mu}(1/q)$$

$$= \sum_{\lambda,\mu \,|\, \mu \subseteq \lambda} q^{n(\lambda)} P_\lambda(zx; q) (1/z)^{|\mu|} C_{\lambda,\mu}(1/q),$$

where we have used the homogeneity of the Hall-Littlewood polynomials and the notation zx for the set of variables $\{zx_i, i \geqslant 1\}$. Therefore we can use (14) with x replaced by zx and z by $1/z$, to get

$$\prod_{i \geqslant 1} \frac{1}{(1-zx_i)(1-zx_i/z)},$$

which is obviously equal to the right-hand side of (14). We thus have the identity

$$\sum_{\lambda,\nu \,|\, \nu \subseteq \lambda} q^{n(\lambda)} P_\lambda(x; q) z^{|\nu|} C_{\lambda,\nu}(1/q) = \sum_{\lambda,\nu \,|\, \nu \subseteq \lambda} q^{n(\lambda)} P_\lambda(x; q) z^{|\lambda|-|\nu|} C_{\lambda,\nu}(1/q),$$

which yields (13), by using the fact that $P_\lambda(x; q)$ is a $\mathbb{Z}[q]$-basis of $\Lambda[q]$ and extracting the coefficient of $z^k q^{n(\lambda)} P_\lambda(x; q)$ on both sides. $\square$

Examples.
1- First, we have $x_1 = R_{1^1} + 1$, and more generally
$$x_n = R_{n^1} + R_{(n-1)^1} + \cdots + R_{1^1} + 1.$$

That is exactly the relation obtained in [Del11] in order to compute the u-average of the function $H \mapsto |H[p^n]|$.

2- One can also see that $x_1^2 = R_{1^2} + (t+1)R_{1^1} + 1$ and that
$$x_1 x_2 = R_{1^1 2^1} + tR_{2^1} + R_{1^2} + (t+1)R_{1^1} + 1.$$

Therefore
$$x_2^2 = R_{2^2} + (t+1)R_{1^1 2^1} + t(t+1)R_{2^1} + R_{1^2} + (t+1)R_{1^1} + 1.$$

3- As we saw the polynomial
$$\sum_{\mu \subseteq \lambda} C_{\lambda,\mu}(t) T^{|\mu|} \in \mathbb{Z}(t)[T]$$

is in fact a self-reciprocal polynomial. Of course, this can be directly checked in the above two examples.

4- Let us consider the case x_1^m. Then the partitions $\mu \subseteq 1^m$ are exactly the partitions 1^k for $k = 0, 1, \ldots, m$. Hence,

$$(15) \qquad\qquad\qquad x_1^m = \sum_{k=0}^m \begin{bmatrix} m \\ k \end{bmatrix}_t R_{1^k}.$$

We will come back later to this example.

Remark. As Ole Warnaar communicated to us, there is an interesting context containing generalizations of Theorems 4 and 5. Indeed, studying properties for Macdonald interpolation polynomials (which are symmetric and whose top homogeneous layer are the classical symmetric Macdonald polynomials, themselves being two parameters generalizations of the Hall-Littlewood polynomials), Okounkov defined in [Oko97] the (q,t)-binomial coefficients $\begin{bmatrix}\lambda\\\mu\end{bmatrix}_{q,t}$, where λ and μ are integer partitions and q, t are complex parameters. These (q,t)-binomial coefficients are defined as quotients of special values of the Macdonald interpolation polynomials, and as remarked by Warnaar, it turns out by using (12) that we have

$$C_{\lambda,\mu}(1/q) = \begin{bmatrix}\lambda\\\mu\end{bmatrix}_{0,q}.$$

Many properties for these (q,t)-binomial coefficients are known, some of which should therefore have interesting algebraic number theoritic applications in our context. As we only need the Hall-Littlewood case for our purpose here, we plan to study further this connection with Macdonald polynomials in a later work. We only mention the following generalization of Theorem 5 (the latter being obtained by setting $\nu = 0$, $q = 0$ and then replacing t by q), which is proved by Lascoux, Rains and Warnaar in [LRW09] (actually in the more general context of nonsymmetric Macdonald interpolation polynomials):

$$\sum_{|\mu|=k} \begin{bmatrix}\lambda\\\mu\end{bmatrix}_{q,t}\begin{bmatrix}\mu\\\nu\end{bmatrix}_{q,t} = \sum_{|\mu|=|\lambda|+|\nu|-k} \begin{bmatrix}\lambda\\\mu\end{bmatrix}_{q,t}\begin{bmatrix}\mu\\\nu\end{bmatrix}_{q,t},$$

where λ and ν are fixed integer partitions. Moreover, still remarked by Warnaar, the inversion in Theorem 4 can also be proved using a $(q \to 0)$ limit case of the inversion for (q,t)-binomial coefficients, which can be found in [Oko97], and can be stated as follows:

$$\sum_{\mu}(-1)^{|\mu|-|\lambda|}q^{n(\mu')-n(\lambda')}t^{n(\lambda)-n(\mu)}\begin{bmatrix}\lambda\\\mu\end{bmatrix}_{q,t}\begin{bmatrix}\mu\\\nu\end{bmatrix}_{1/q,1/t} = \delta_{\lambda,\nu},$$

where $\delta_{\lambda,\nu}$ stands for the Kronecker symbol.

5. Links with finite abelian groups

5.1. **Finite abelian p-groups and the polynomial R_λ.** We have already seen in the previous section that the inversion we needed for our computations of u-averages is related to finite abelian p-groups, through the coefficients $C_{\lambda,\mu}$. We highlight here this link. There is a classical bijection between the set of partitions of a fixed nonnegative integer m and the isomorphism classes of finite abelian p-groups of order p^m. Indeed, to any partition $\lambda = 1^{m_1}2^{m_2}\cdots\ell^{m_\ell}$ of m, we associate the finite abelian p-group

$$H_\lambda = (\mathbb{Z}/p\mathbb{Z})^{m_1} \oplus (\mathbb{Z}/p^2\mathbb{Z})^{m_2} \oplus \cdots \oplus (\mathbb{Z}/p^\ell\mathbb{Z})^{m_\ell}.$$

Recall that $\lambda'_1, \lambda'_2, \ldots, \lambda'_\ell$ denote the parts of the conjugate of λ (therefore $\lambda'_i = \sum_{j\geqslant i} m_j$), and we have (see [CL84])

$$(16) \qquad |\mathrm{Aut}(H_\lambda)| = p^{\lambda_1'^2+\lambda_2'^2+\cdots+\lambda_\ell'^2}\prod_{j=1}^{\ell}(1/p; 1/p)_{m_j}.$$

Furthermore if $G_\lambda \simeq H_\lambda \times H_\lambda$ is a group of type S, we have (see [Del01]):

$$|\operatorname{Aut}^s(G_\lambda)| = p^{2(\lambda_1'^2 + \lambda_2'^2 + \cdots + \lambda_\ell'^2) + m} \prod_{j=1}^{\ell} (1/p^2; 1/p^2)_{m_j}.$$

Remark also that we have

$$H_\lambda[p^k] \simeq (\mathbb{Z}/p\mathbb{Z})^{m_1} \oplus (\mathbb{Z}/p^2\mathbb{Z})^{m_2} \oplus \cdots \oplus (\mathbb{Z}/p^{k-1}\mathbb{Z})^{m_{k-1}} \oplus (\mathbb{Z}/p^k\mathbb{Z})^{\lambda_k'},$$

hence

(17)
$$|H_\lambda[p^k]| = p^{\lambda_1' + \cdots + \lambda_k'}.$$

The following definitions will be useful in the sequel.

Definition 6. *For a set of ℓ variables $x = \{x_1, \ldots, x_\ell\}$, let $T(x) = T(x_1, \ldots, x_\ell)$ be a polynomial and H be a finite abelian p-group. We define*

$$T(H) = T(|H[p]|, |H[p^2]|, \ldots, |H[p^\ell]|).$$

Definition 7. *If $\mu = 1^{n_1} 2^{n_2} \cdots \ell^{n_\ell}$ is an integer partition, we denote by x^μ the following monomial*

$$x^\mu := x_1^{n_1} x_2^{n_2} \cdots x_\ell^{n_\ell}.$$

Hence, with these definitions, the u-average of $|H[p^\ell]|$ can be simply written as $\mathrm{M}_u(x_\ell)$. More generally, the u-average of $|H[p]|^{n_1} |H[p^2]|^{n_2} \cdots |H[p^\ell]|^{n_\ell}$ is simply $\mathrm{M}_u(x^\mu)$ where μ denotes the integer partition $\mu = 1^{n_1} 2^{n_2} \cdots \ell^{n_\ell}$.

In order to give a closed formula for the latter, we state the following result.

Theorem 8. *For a positive integer ℓ, let $\lambda = 1^{m_1} 2^{m_2} \cdots \ell^{m_\ell}$ be an integer partition and let H be a finite abelian p-group. Then the number of injective homomorphisms of H_λ into H is given by*

$$\prod_{i=1}^{\ell} \prod_{j=\lambda_{i+1}'}^{\lambda_i' - 1} \left(|H[p^i]| - p^j |H[p^{i-1}]| \right),$$

or in other words,

$$\left| \{ \operatorname{Hom}_{\mathrm{inj}}(H_\lambda, H) \} \right| = R_\lambda(H; p).$$

Proof. This is probably a known formula that can be found in the literature, however we give here a sketch of proof. Write

$$H_\lambda = (\mathbb{Z}/p\mathbb{Z})^{m_1} \oplus \left(\mathbb{Z}/p^2\mathbb{Z} \right)^{m_2} \oplus \cdots \oplus \left(\mathbb{Z}/p^\ell\mathbb{Z} \right)^{m_\ell},$$

and take $e_1, e_2, \cdots, e_{\lambda_1'}$ a "canonical basis" in an obvious sense so that $e_1, \ldots, e_{m_1}$ are of order p and $e_{m_1 + m_2 + \cdots + m_{\ell-1} + 1}, \ldots, e_{\lambda_1'}$ are or order p^ℓ. In order to define an injective homomorphism of H_λ into H, we need to specify the image f_i of each e_i. The image, $f_{\lambda_1'}$ of $e_{\lambda_1'}$ is any point of order p^ℓ and there are $|H[p^\ell]| - |H[p^{\ell-1}]|$ choices for this image (these correspond to the factor $i = \ell$ and $j = 0 = \lambda_{\ell+1}'$ in the theorem). Assume that $k + 1 \leqslant \lambda_1'$, and that $f_{\lambda_1'}, \ldots, f_{k+1}$ are already defined. Let p^t be the order of e_k. Note that the order of each $f_{\lambda_1'}, \ldots, f_{k+1}$ is $\geqslant p^t$. Now the image f_k of e_k must be an element of order p^t such that, for any $r = 1, \ldots, p^t - 1$, $r f_k$ is not in the subgroup $\langle f_{k+1}, \ldots, f_{\lambda_1'} \rangle$ generated by the images that are already defined. The latter means that the image of f_k in the quotient group $\tilde{H} = H / \langle f_{k+1}, \ldots, f_{\lambda_1'} \rangle$ has order p^t. The number of elements of order p^t in $\tilde{H}$ is $|\tilde{H}[p^t]| - |\tilde{H}[p^{t-1}]|$. For each of these elements there are $|\langle f_{k+1}, \ldots, f_{\lambda_1'} \rangle[p^t]|$ corresponding pre-images of order p^t in H. Hence the number of possibilities for f_k is

$$\left(|\tilde{H}[p^t]| - |\tilde{H}[p^{t-1}]| \right) |\langle f_{k+1}, \ldots, f_{\lambda_1'} \rangle[p^t]| = |H[p^t]| - p^{\lambda_i' - k} |H[p^{t-1}]|.$$

This is exactly the factor ocurring with $i = k$ in the formula of the theorem. $\square$

We derive the following consequence.

Corollary 9. *Let n and m be nonnegative integers, and λ be a fixed partition of m. Then we have*

$$\sum_{\mu \vdash n} \frac{R_\lambda(H_\mu; p)}{|\operatorname{Aut} H_\mu|} = \frac{1}{p^{n-m}(1/p; 1/p)_{n-m}},$$

which can equivalently be written as follows in terms of generating functions

$$\sum_{n \geqslant 0} z^n \sum_{\mu \vdash n} \frac{R_\lambda(H_\mu; p)}{|\operatorname{Aut} H_\mu|} = \frac{z^m}{(z/p; 1/p)_\infty}.$$

Proof. We clearly have

$$|\operatorname{Hom}_{\mathrm{inj}}(H_\lambda, H)| = |\operatorname{Aut}(H_\lambda)| \cdot |\{J \text{ subgroup of } H, J \simeq H_\lambda\}|.$$

Then Proposition 4.1 of [CL84] gives

$$|\operatorname{Aut}(H_\lambda)| \sum_{H(p^n)} \frac{|\{J \text{ subgroup of } H, J \simeq H_\lambda\}|}{|\operatorname{Aut}(H)|} = \frac{1}{p^{n-m}(1/p; 1/p)_{n-m}}.$$

We obtain the first equality from the correspondence $(\mu \vdash n) \leftrightarrow (H_\mu \text{ of order } p^n)$. The second equality comes from Euler's identity (see for instance [GR04])

$$\sum_{n \geqslant m} \frac{z^n}{p^{n-m}(1/p; 1; p)_{n-m}} = z^m \sum_{n \geqslant 0} \frac{z^n}{p^n(1/p; 1; p)_n}$$

$$= z^m \frac{1}{(z/p; 1/p)_\infty}.$$

$\square$

Using Theorem 5, Definition 7, and Corollary 9, we obtain the following result.

Theorem 10. *Let λ be a fixed integer partition, and z a complex number. We have*

$$\sum_\mu \frac{x^\lambda(H_\mu)}{|\operatorname{Aut} H_\mu|} z^{|\mu|} = \frac{1}{(z/p; 1/p)_\infty} \sum_{\nu \subseteq \lambda} C_{\lambda,\nu}(p) \, z^{|\nu|},$$

where the sum on the left-hand side is over all integer partitions μ, and the sum on the right-hand side is over all partitions ν satisfying $\nu_i \leqslant \lambda_i$ for all i.

5.2. **A combinatorial formula.** As a consequence in combinatorics, we derive the following by setting $q = 1/p$ and switching μ into μ' in Theorem 10, and finally using (16) and (17).

Corollary 11. *For a positive integer ℓ, let $\lambda = 1^{m_1} 2^{m_2} \cdots \ell^{m_\ell}$ be a fixed integer partition, and z be a complex number. We have:*

$$(18) \qquad \sum_\mu \frac{q^{\sum_{i \geqslant 1} \mu_i^2} q^{-m_1 \mu_1 - \cdots - m_\ell(\mu_1 + \cdots + \mu_\ell)}}{b_\mu(q)} z^{|\mu|} = \frac{1}{(zq)_\infty} \sum_{\nu \subseteq \lambda} C_{\lambda,\nu}(1/q) \, z^{|\nu|}.$$

This identity generalizes [Del11, corollary 4], and we give here an alternative proof through Lascoux's formula (5), without using the previous computations for finite abelian groups. First, it is possible to rewrite the left-hand side of (18) with the

notations of Hall-Littlewood functions. Indeed, replace μ by its conjugate μ' on the left-hand side, note that

$$
\begin{aligned}
\sum_{i=1}^{\ell} m_i(\mu'_1 + \cdots + \mu'_i) &= \sum_{i=1}^{\ell}(\lambda'_i - \lambda'_{i+1})(\mu'_1 + \cdots + \mu'_i) \\
&= \sum_{i=1}^{\ell} \lambda'_i \mu'_i = (\lambda'|\mu'),
\end{aligned}
$$

and write

$$
\sum_{i \geqslant 1} \mu'^2_i = 2n(\mu) + |\mu|.
$$

Then, using the limit case $n \to \infty$ of the specialization (2), we can rewrite (18) in the following way:

$$
(19) \qquad \sum_{\mu} q^{|\mu|+n(\mu)-(\lambda'|\mu')} P_{\mu}(z, zq \ldots; q) = \frac{1}{(zq)_{\infty}} \sum_{\nu \subseteq \lambda} C_{\lambda,\nu}(1/q)\, z^{|\nu|}.
$$

Now multiply both sides of (19) by $q^{n(\lambda)} P_{\lambda}(x; q)$ and sum over all partitions λ. As Hall-Littlewood functions form a $\mathbb{Z}[q]$-basis of $\Lambda[q]$, it is enough to show that

$$
(20) \quad \sum_{\lambda,\mu} q^{n(\lambda)+n(\mu)-(\lambda'|\mu')} P_{\lambda}(x; q) P_{\mu}(zq, zq^2 \ldots; q)
$$

$$
= \frac{1}{(zq)_{\infty}} \sum_{\nu \subseteq \lambda} q^{n(\lambda)} P_{\lambda}(x; q) C_{\lambda,\nu}(1/q)\, z^{|\nu|}.
$$

Set $y = \{zq, zq^2, \ldots\}$ in Warnaar's special case (4) of Lascoux's identity to see that the left-hand side of (20) is equal to

$$
\frac{1}{(zq)_{\infty}} \prod_{i \geqslant 1} \frac{1}{(1-x_i)(1-zx_i)},
$$

which, through the generating function (14), is easily seen to be equal to the right-hand side of (20).

5.3. **Consequences on u-averages and proof of Theorem 1.** Using Theorem 10 above, replacing z by p^{-u}, and recalling the definitions of u-averages, we obtain the following u-average on finite abelian p-groups and on p-groups of type S.

Theorem 12. *For a positive integer ℓ, let $\lambda = 1^{m_1} 2^{m_2} \cdots \ell^{m_\ell}$ be an integer partition. Then, the u-average of the function $x^{\lambda} \colon H \mapsto |H[p]|^{m_1} |H[p^2]|^{m_2} \cdots |H[p^{\ell}]|^{m_\ell}$ is equal to*

$$
M_u(x^{\lambda}) = \sum_{\mu \subseteq \lambda} C_{\lambda,\mu}(p) p^{-|\mu|u},
$$

and the u-average of the function x^{λ} in the sense of groups of type S is equal to

$$
M_u^S(x^{\lambda}) = \sum_{\mu \subseteq \lambda} C_{\lambda,\mu}(p^2) p^{-|\mu|(2u-1)}.
$$

Theorem 5 implies directly that if $\lambda = 1^{m_1} 2^{m_2} \cdots \ell^{m_\ell}$ is an integer partition, then we have

$$
M_0^s(x^{\lambda}) = M_1^s(x^{\lambda})\, p^{m_1 + 2m_2 + \cdots + \ell m_\ell},
$$

which is exactly Theorem 1.

6. Consequence on the heuristics on class groups and on Tate-Shafarevich groups

6.1. **Class groups of quadratic number fields.** The Cohen-Lenstra heuristics ([CL84]) allow to give precise conjectures for the behavior of the class groups of number fields varying in natural families. Here, we only recall briefly the Cohen heuristics in the case of families of quadratic number fields. For $K_d = \mathbb{Q}(\sqrt{d})$ a quadratic number field with discriminant d, we denote by $\mathrm{C}\ell(d)$ its class group so that $\mathrm{C}\ell(d)_p$ is its p-part. First, take the family of imaginary quadratic number fields: these are the fields K_d where $d < 0$ runs through the whole set of fundamental negative discriminants. Assume that $p \geqslant 3$ (actually, the 2-part of the class groups of quadratic fields behaves in a specific and well-understood way, due to the genus theory, [Coh93]). If h is a "reasonable" function defined over finite abelian p-groups, then the Cohen-Lenstra heuristics predict that the average of h over the p-part of the class group $\mathrm{C}\ell(d)_p$ is the 0-average of h (0 being the rank of the group of units of K_d), that is, we should have

$$\lim_{X \to \infty} \frac{\displaystyle\sum_{|d| \leqslant X,\, d<0} h(\mathrm{C}\ell(d)_p)}{\displaystyle\sum_{|d| \leqslant X,\, d<0} 1} = \mathrm{M}_0(h).$$

For the family of real quadratic number fields, i.e., fields K_d where $d > 0$ runs through the set of fundamental positive discriminants, the Cohen-Lenstra heuristics predict that the average of h over the p-part of the class group $\mathrm{C}\ell(d)_p$ is the 1-average of h (1 being, in that case, the rank of $U(K)$), that is, we should have:

$$\lim_{X \to \infty} \frac{\displaystyle\sum_{|d| \leqslant X,\, d>0} h(\mathrm{C}\ell(d)_p)}{\displaystyle\sum_{|d| \leqslant X,\, d>0} 1} = \mathrm{M}_1(h).$$

There are strong evidence and numerical data supporting the heuristic principle, however only few results are proved. The first one is for $p = 3$ and the function $h(H) = |H[3]|$, the number of 3-torsion elements in H. Davenport and Heilbronn ([DH71]) proved (before the heuristics were formulated) that the average over the 3-part of the class groups of the function h is equal to 2 (resp. 4/3) in the case of imaginary (resp. real) quadratic fields. In their paper, Cohen and Lenstra proved (it is not a trivial result) that $\mathrm{M}_0(h) = 2$ and $\mathrm{M}_1(h) = 4/3$. There are other results in the literature for other families of number fields, and for the 4-part of class groups of quadratic number fields ([Bha05], [FK07]).

Of course, the case $p = 3$ and the function $H \mapsto |H[3]|$ is a particular case of our work. Now, from our computations, we can predict the average of all the moments of the number of p^ℓ-torsion elements in the class groups.

Conjecture 1. *For any positive integer ℓ, let $\lambda = 1^{m_1} 2^{m_2} \cdots \ell^{m_\ell}$ be an integer partition, and assume that $p \geqslant 3$.*
As d is varying over the set of fundamental negative discriminants the average of $|\mathrm{C}\ell(d)[p]|^{m_1} |\mathrm{C}\ell(d)[p^2]|^{m_2} \cdots |\mathrm{C}\ell(d)[p^\ell]|^{m_\ell}$ is equal to

$$\sum_{\mu \subseteq \lambda} C_{\lambda,\mu}(p).$$

As d is varying over the set of fundamental positive discriminants the average of $|\operatorname{C}\!\ell(d)[p]|^{m_1}|\operatorname{C}\!\ell(d)[p^2]|^{m_2}\cdots|\operatorname{C}\!\ell(d)[p^\ell]|^{m_\ell}$ *is equal to*

$$\sum_{\mu\subseteq\lambda} C_{\lambda,\mu}(p)p^{-|\mu|}.$$

In particular, (still for $p\neq 2$) and using equation (15), one obtains that the average of $|\operatorname{C}\!\ell(d)[p]|^n$ of class group of imaginary (resp. real) quadratic fields is equal to

$$M_0(x^{1^n}) = \sum_{k=0}^{n}\begin{bmatrix}n\\k\end{bmatrix}_p \quad \left(\text{resp. } M_1(x^{1^n}) = \frac{1}{p}\sum_{k=0}^{n}\begin{bmatrix}n\\k\end{bmatrix}_p\right)$$

Those are exactly the $\mathcal{N}(n,p)$ (resp. $\mathcal{M}_n(p)$) used in [FK07, FK06]. In particular, Fouvry and Klueners used $\mathcal{N}(n,p)$ (resp. $\mathcal{M}_n(p)$) in [FK06] in order to prove that conjectures (coming from a special case of the Cohen-Lenstra heuristics) related to the moments of the number of p-torsion points in class groups imply conjectures (coming from another special case of the Cohen-Lenstra heuristics) about the probability laws of the p-ranks of the class groups. Our results could be used to generalize their results and also to adapt them in the case of Tate-Shafarevich groups. This will be explained in a forthcoming paper.

6.2. **Tate-Shafarevich groups of elliptic curves.** Let $u \geqslant 0$ be a fixed integer, and consider the family $\mathcal{F}$ of elliptic curves E defined over $\mathbb{Q}$, with rank u, and ordered by the conductor N_E. The Tate-Shafarevich group $\text{Ш}(E)$ is conjecturally a finite abelian group. If so, then $\text{Ш}(E)$ is a group of type S. The heuristic principle ([Del01, Del07]) asserts that if g is a "reasonable" function defined over isomorphism classes of p-group of type S, we should have

$$\lim_{X\to\infty}\frac{\displaystyle\sum_{E\in\mathcal{F},\,N_E\leqslant X}g(\text{Ш}(E)_p)}{\displaystyle\sum_{E\in\mathcal{F},\,N_E\leqslant X}1} = \text{M}_u^s(g).$$

Important remark and correction of the first version of the heuristics on Tate-Shafarevich groups. In this paper, the heuristics on Tate-Shafarevich groups, in particular the equation above and Conjecture 2 take into account the following correction. Due to a bad choice of a parameter, the heuristic assumption for Tate-Shafarevich groups stated in [Del01] is wrong and should be corrected for $u > 0$ by the following: in the Heuristic Assumption of [Del01, page 195], the equality $M_u(f) = M_{u/2}^s(f)$ *must be replaced by* $M_u(f) = M_u^s(f)$ (hence, the examples given should also be modified in consequence). Note that this was done in [Del07] but only explicitly for rank 1 elliptic curves. In fact, this correction was suggested by Kowalski observing that only the corrected version of the heuristics is compatible with results of Heath-Brown ([HB94, HB93]) on the 2-rank of the Selmer groups of the family of elliptic curves $E_d\colon y^2 = x^3 - d^2x$, d odd and squarefree (see [Kow07, Remark 2.6]). Note that this corrected version is also compatible with other theoretical results and conjectural works, see the discussion after Conjecture 2.

The heuristic principle has many applications and there are numerical evidence supporting them. With our previous computations on u-averages for groups of type S we are led to conjecture the following.

Conjecture 2. *For any positive integer ℓ, let $\lambda = 1^{m_1}2^{m_2}\cdots\ell^{m_\ell}$ be an integer partition, and let $u \geqslant 0$ be an integer. As $E/\mathbb{Q}$, ordered by conductors, is varying over*

elliptic curves with rank u, the average of $|\mathrm{III}(E)[p]|^{m_1}|\mathrm{III}(E)[p^2]|^{m_2}\cdots|\mathrm{III}(E)[p^{\ell}]|^{m_{\ell}}$ is equal to

$$\sum_{\mu\subseteq\lambda} C_{\lambda,\mu}(p^2)p^{-|\mu|(2u-1)}.$$

In particular, if we take the function g such that $g(G) = |G[p^{\ell}]|$ then we have:

$$\mathrm{M}_u^s(g) = 1 + \frac{1}{p^{2u-1}} + \cdots + \frac{1}{p^{(2u-1)\ell}},$$

which for instance, when $\ell = 1$, gives $\mathrm{M}_0^s(g) = 1 + p$ and $\mathrm{M}_1^s(g) = 1 + 1/p$.

The rank conjecture in its strong form (asserting that the rank of E is 0 or 1 with probability $1/2$ each and that elliptic curves with rank $\geqslant 2$ do not contribute in the averages), and the results of Bhargava and Shankar [BS10b, BS10a], imply that the average size over all elliptic curves $E/\mathbb{Q}$ with rank 0 (resp. rank 1) of $\mathrm{III}(E)[p]$ is $1 + p$ (resp. $1 + 1/p$) for $p = 2$ and $p = 3$. From their work, Bhargava and Shankar also made a conjecture for all p which, together with the rank conjecture, would imply that the average size $|\mathrm{III}(E)[p]|$ is $1 + p$ (resp. $1 + 1/p$) for rank 0 (resp. rank 1) elliptic curves.

Swinnerton-Dyer [SD08] and Kane [Kan11] obtained results for $p = 2$ and for the family of quadratic twists, E_d, of any fixed elliptic curve $E/\mathbb{Q}$ with $E[2] \subset E(\mathbb{Q})$ and having no rational cyclic subgroup of order 4. Their results and the rank conjecture imply that the average of $|\mathrm{III}(E_d)[2]|$ is 3 (resp. $3/2$) for the rank 0 (resp. rank 1) curves. There are also in the literature some other theoretical results for other families of elliptic curves, mainly for $p = 2$.

Actually, all the previous theoretical results are directly concerned with the behavior of p-Selmer groups of elliptic curves. If $n \in \mathbb{N}$, the n-Selmer group $\mathrm{Sel}_n(E)$ and the Tate-Shafarevich group of an elliptic curve are linked by the exact sequence

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to \mathrm{Sel}_n(E) \to \mathrm{III}(E)[n] \to 0.$$

So, if $E(\mathbb{Q})_{\mathrm{tors}} = 0$ and if the rank of E is u, then we have $|\mathrm{Sel}_n(E)| = n^u|\mathrm{III}(E)[n]|$. Therefore, assuming the rank conjecture, any result on $\mathrm{Sel}_n(E)$ gives an information on $\mathrm{III}(E)[n]$. Reciprocally, the distribution of $\mathrm{Sel}_n(E)$ can be deduced from the distribution of $\mathrm{III}(E)[n]$ for rank 0 and rank 1 curves.

Recently, Poonen and Rains [PR12] gave a very deep model for the behavior of the p-Selmer groups of all elliptic curves (they do not separate elliptic curves by their rank). In particular, they obtained the following predictions for elliptic curves defined over $\mathbb{Q}$.

Conjecture 3 (Poonen-Rains). *For any integer $m \geqslant 0$, the average of $|\mathrm{Sel}_p(E)|^m$ over all $E/\mathbb{Q}$ is equal to $\prod_{j=1}^{m}(1 + p^j)$.*

Assuming that the p-parts of $\mathrm{Sel}_n(E)$ behave independently for $p|n$, except for the constraint that their parities are equal, they obtained a conjecture for the average of $|\mathrm{Sel}_n(E)|^m$ for all squarefree positive integer n. The Poonen and Rains model suggests that the p-Selmer groups behave in the same way for rank 0 and rank 1 elliptic curves. If we assume that elliptic curves of rank $\geqslant 2$ do not contribute to the average value, then this is also suggested by the heuristic principle since $E(\mathbb{Q})_{\mathrm{tors}} = 0$ with probability 1 and $\mathrm{M}_0^s(g) = \mathrm{M}_1^s(g)p$ (recall that here, g denotes the function $G \mapsto |G[p]|$). It is then natural to ask wether this is still true for all integers n, without the squarefree restriction. Theorem 1 and the discussions above suggest that this is indeed the case, yielding the following conjecture.

Conjecture 4. *Let $\ell \geqslant 1$ and $m \geqslant 0$ be integers. The average of $|\operatorname{Sel}_{p^\ell}(E)|^m$ over all $E/\mathbb{Q}$ is equal to*

$$\sum_{\mu \subseteq \lambda} C_{\lambda,\mu}(p^2) p^{|\mu|}$$

where λ is the integer partition $\lambda = \ell^m$.

For $\ell = 1$, equation (15) gives $\sum_{\mu \subseteq \lambda} C_{\lambda,\mu}(p^2) p^{|\mu|} = \sum_{k=0}^{m} \left[\begin{smallmatrix} m \\ k \end{smallmatrix}\right]_{p^2} p^k$. It can be easily shown that the last sum is indeed equal to $\prod_{j=1}^{m}(1+p^j)$, as claimed in Conjecture 3.

One can clarify the links between the different conjectures involved in the discussion above. If E is an elliptic curve over $\mathbb{Q}$, we denote by $\operatorname{rk}(E)$ the rank of its Mordell-Weil group. We have in mind:

- The rank conjecture asserting that $\operatorname{rk}(E)$ is 0 or 1 with probability 1/2 each.
- The assumption saying that elliptic curves of rank $\geqslant 2$ contribute nothing to the average value of $p^{m\,\operatorname{rk}(E)}$. Note that this depends on m, therefore we denote by $e_{p,m}$ the lim sup, as $N \to \infty$, of the sum of $p^{m\,\operatorname{rk}(E)}$ over curves of rank $\geqslant 2$ and conductor $\leqslant N$, divided by the total number of curves of conductor $\leqslant N$.
- The Poonen-Rains conjecture (Conjecture 1.1 in [PR12]).
- The heuristic model for the probability laws $\dim_{\mathbb{F}_p} \operatorname{III}(E)[p]$ ([Del01, Del07]).
- The heuristic model for the moment of $\operatorname{III}(E)$, i.e., Conjecture 2 for an integer partition λ.

As discussed above and also explained in [PR12], the rank conjecture and Conjecture 1.1 in [PR12] imply the heuristic model for $\dim_{\mathbb{F}_p} \operatorname{III}(E)[p]$, and so Conjecture 2 for $|\operatorname{III}(E)[p]|^m$ (i.e., $\lambda = 1^m$) for rank 0 and rank 1 curves.

Also, Poonen and Rains proved ([PR12, Theorem 5.2]) that the rank conjecture is the only distribution on $\operatorname{rk}(E)$ compatible with the Poonen-Rains conjecture and the heuristic model for $\dim_{\mathbb{F}_p} \operatorname{III}(E)[p]$.

Furthermore, Conjecture 1.1 in [PR12] also implies that $e_{p,m} = 0$ for $m = 1, 2, 3$ (in fact, Poonen and Rains prove it for $m = 1$ but their argument can be directly adapted for $m = 2$ and $m = 3$).

On the other hand, one can see that the equality $e_{p,m} = 0$, the rank conjecture, and Conjecture 2 for the moments of $|\operatorname{III}(E)[p^\ell]|^m$ (strengthening with the assumption that the error terms implied in the averages are uniformly bounded independently of the rank u), imply Conjecture 4. Indeed (for simplicity we restrict the following computations to elliptic curves E such that $E(\mathbb{Q})_{\mathrm{tors}} = \{0\}$), we first see that

$$\sum_{\substack{N_E \leqslant X \\ \operatorname{rk}(E) \geqslant 2}} |\operatorname{Sel}_{p^\ell}(E)|^m = \sum_{u \geqslant 2} p^{mu} \frac{\displaystyle\sum_{\substack{N_E \leqslant X \\ \operatorname{rk}(E) = u}} |\operatorname{III}(E)[p^\ell]|^m}{\displaystyle\sum_{\substack{N_E \leqslant X \\ \operatorname{rk}(E) = u}} 1} \sum_{\substack{N_E \leqslant X \\ \operatorname{rk}(E) = u}} 1.$$

Now, the fraction in the sum of the right-hand side tends to $\mathrm{M}_u^s(x^{\ell^m})$ as $X \to \infty$. Using the fact that $u \mapsto \mathrm{M}_u^s(x^{\ell^m})$ is decreasing (because the coefficients $C_{\lambda,\mu}$ are positive) and the above assumption on the error terms, we deduce that this fraction

is uniformly bounded (and the bound does not depend on u). Hence,

$$\sum_{\substack{N_E \leqslant X \\ \mathrm{rk}(E) \geqslant 2}} |\operatorname{Sel}_{p^\ell}(E)|^m = O\left(\sum_{\substack{N_E \leqslant X \\ \mathrm{rk}(E) \geqslant 2}} p^{m\,\mathrm{rk}(E)}\right).$$

Therefore, since by assumption $e_{p,m} = 0$, we deduce that the average of $|\operatorname{Sel}_{p^\ell}(E)|^m$ of curves E of rank $\geqslant 2$ among all elliptic curves is equal to 0. Now, we can write

$$
\frac{\displaystyle\sum_{N_E \leqslant X} |\operatorname{Sel}_{p^\ell}(E)|^m}{\displaystyle\sum_{N_E \leqslant X} 1} = \frac{\displaystyle\sum_{\substack{N_E \leqslant X \\ \mathrm{rk}(E)=0}} |\operatorname{Sel}_{p^\ell}(E)|^m}{\displaystyle\sum_{\substack{N_E \leqslant X \\ \mathrm{rk}(E)=0}} 1} \cdot \frac{\displaystyle\sum_{\substack{N_E \leqslant X \\ \mathrm{rk}(E)=0}} 1}{\displaystyle\sum_{N_E \leqslant X} 1}
$$

$$
+ \frac{\displaystyle\sum_{\substack{N_E \leqslant X \\ \mathrm{rk}(E)=1}} |\operatorname{Sel}_{p^\ell}(E)|^m}{\displaystyle\sum_{\substack{N_E \leqslant X \\ \mathrm{rk}(E)=1}} 1} \cdot \frac{\displaystyle\sum_{\substack{N_E \leqslant X \\ \mathrm{rk}(E)=1}} 1}{\displaystyle\sum_{N_E \leqslant X} 1} + \frac{\displaystyle\sum_{\substack{N_E \leqslant X \\ \mathrm{rk}(E) \geqslant 2}} |\operatorname{Sel}_{p^\ell}(E)|^m}{\displaystyle\sum_{N_E \leqslant X} 1}.
$$

The last term on the right-hand side tends to 0 as $X \to \infty$. Now, replace $|\operatorname{Sel}_{p^\ell}|$ by $|Ш(E)[p^\ell]|$ in the first term and $|\operatorname{Sel}_{p^\ell}|$ by $p^\ell|Ш(E)[p^\ell]|$ in the second one and use Conjecture 2, Theorem 1 and the rank conjecture to conclude.

Remark. In the above discussions, one can replace the number field $\mathbb{Q}$ by an arbitrary number field K.

7. u-AVERAGES AND HALL-LITTLEWOOD POLYNOMIALS

7.1. u-**averages and combinatorial consequences.** In the paper [Del11], the first author computed the u-probabilities laws for the p^j-ranks of finite abelian p-groups (recall that the p^j-rank of H is the dimension over $\mathbb{F}_p$ of the vector space $p^{j-1}H/p^j H$ and is denoted $r_{p^j}(H)$), which we rewrite below.

Proposition 13 (Corollary 11 of [Del11]). *Let $\ell \geqslant 1$ be an integer and μ be an integer partition with $\ell(\mu) \leqslant \ell$ (here μ is given by its parts $\mu_1 \geqslant \mu_2 \geqslant \cdots \geqslant \mu_\ell \geqslant 0$). Then the u-probability that a finite abelian p-group has its p^j-rank equal to μ_j for all $1 \leqslant j \leqslant \ell$ is equal to*

$$\frac{\prod_{j \geqslant \mu_\ell + 1}(1 - 1/p^{u+j})}{p^{\mu_1^2 + \cdots + \mu_\ell^2 + u(\mu_1 + \cdots + \mu_\ell)} \prod_{j=1}^{\ell}(1/p; 1/p)_{\mu_j - \mu_{j+1}}},$$

and the u-probability that a group of type S has its p^j-rank equal to $2\mu_j$ for all $1 \leqslant j \leqslant \ell$ is equal to

$$\frac{\prod_{j \geqslant \mu_\ell + 1}(1 - 1/p^{2u+2j-1})}{p^{2(\mu_1^2 + \cdots + \mu_\ell^2) + (2u-1)(\mu_1 + \cdots + \mu_\ell)} \prod_{j=1}^{\ell}(1/p^2; 1/p^2)_{\mu_j - \mu_{j+1}}}.$$

Hence, for a fixed integer partition $\lambda = 1^{m_1} 2^{m_2} \cdots \ell^{m_\ell}$, we can also compute the u-average of x^λ over finite abelian p-groups (with the notations of Theorem 12) by its moments. Indeed, we have

$$x^\lambda(H) = p^{r_p(H)m_1 + (r_p(H) + r_{p^2}(H))m_2 + \cdots + (r_p(H) + \cdots + r_{p^\ell}(H))m_\ell},$$

therefore

$$M_u(x^\lambda) = \sum_{0 \leqslant \mu_\ell \leqslant \cdots \leqslant \mu_1} u\text{-prob}(r_p(H) = \mu_1, \ldots, r_{p^\ell}(H) = \mu_\ell) p^{\mu_1 m_1 + \cdots + (\mu_1 + \cdots + \mu_\ell) m_\ell}.$$

Replacing u-prob$(r_p(H) = \mu_1, \ldots, r_{p^\ell}(H) = \mu_\ell)$ by the value given in Proposition 13 and $M_u(x^\lambda)$ by its value from Theorem 12, we obtain

$$\sum_{\ell(\mu) \leqslant \ell} \frac{\prod_{j \geqslant \mu_\ell + 1}(1 - 1/p^{u+j})}{p^{\mu_1^2 + \cdots + \mu_\ell^2 + u(\mu_1 + \cdots + \mu_\ell)} \prod_{j=1}^{\ell}(1/p; 1/p)_{\mu_j - \mu_{j+1}}} p^{(\lambda'|\mu)} = \sum_{\nu \subseteq \lambda} C_{\lambda,\nu}(p) p^{-|\nu|u}.$$

By setting $q = 1/p$, replacing μ by its conjugate μ' on the left-hand side, and setting $z = q^{-u}$, we see that this formula is equivalent to the following combinatorial identity.

Theorem 14. *For any nonnegative integer ℓ, let $\lambda = 1^{m_1} 2^{m_2} \cdots \ell^{m_\ell}$ be a fixed integer partition such that $\lambda_1 \leqslant \ell$ (equivalently $\ell(\lambda') \leqslant \ell$), and z be a complex number. Then we have*

$$(21) \qquad \sum_{\mu_1 \leqslant \ell} \frac{z^{|\mu|} q^{2n(\mu) + |\mu| - (\lambda'|\mu')}}{b_\mu(q)} (zq^{\mu'_\ell + 1})_\infty = \sum_{\nu \subseteq \lambda} C_{\lambda,\nu}(1/q) z^{|\nu|}.$$

Remark. One can also replace finite abelian p-groups by groups of type S in the previous discussion. We obtain as a consequence the same combinatorial identity as (21), in which q is replaced by q^2 and then z is replaced by z^2/q.

Note that thanks to Theorem 5, the sum $\sum_{\nu \subseteq \lambda} C_{\lambda,\nu}(1/q) q^{-|\nu|u}$ must be equal to $q^{-|\lambda|u} \sum_{\nu \subseteq \lambda} C_{\lambda,\nu}(1/q) q^{|\nu|u}$. By using (21) with $z = q^{-u}$ and $z = q^u$, this yields an identity between the left-hand sides which seems quite mysterious.

In the case where $m_1 = m_2 = \cdots = m_{\ell-1} = 0$ and $m_\ell = 1$ (therefore $\lambda = (\ell)$, a row partition), identity (21) corresponds to [Del11, Corollary 12], which can be written as follows

$$(22) \qquad \sum_{\mu_1 \leqslant \ell} \frac{z^{|\mu|} q^{2n(\mu)}}{b_\mu(q)} (zq^{\mu'_\ell + 1})_\infty = \frac{1 - z^{\ell+1}}{1 - z}.$$

In view of the structure of (21), it would be a challenging problem to prove it through the theory of Hall-Littlewood functions, by using Warnaar's identity (4) or Lascoux's generalization (5), as we did for proving the symmetry property (13). However, problems occur as we need to bound the first part of the partition μ on the left-hand side in (21), therefore a finite summation of Hall-Littlewood polynomials seems to be required (i.e., a summation over partitions where both the length and the first part are bounded). In his paper [War06], Warnaar raises the question of finding a finite form of (4), which seems out of reach, and therefore finding a finite form of Lascoux's identity seems hopeless. Note that in (4), specializing the variables y_i to 0, one recovers the special case $a = 0$ of (3), for which Warnaar proves a finite version in [War06, Theorem 6.1]. Unfortunately, the latter neither contains (21) nor even (22) as special cases. Inspired by Macdonald's partial fraction method [Mac95] used in [Ste90, JZ05, IJZ06, War06], we can prove the following finite form of (3), which will be shown to contain (22) as a special case.

Theorem 15. *Let n be a positive integer, and $x = \{x_1, \ldots, x_n\}$ be a set of n variables. Then for any complex number a and any positive integer k, we have*

$$(23) \quad \sum_{\lambda \subseteq (k^n)} q^{n(\lambda)}(a;q^{-1})_{\ell(\lambda)}(a;q^{-1})_{n-m_k(\lambda)} P_\lambda(x;q)$$

$$= \sum_{I \subseteq [n]} q^{k\binom{|I|}{2}}(a;q^{-1})_{|I|}(a;q^{-1})_{n-|I|} \prod_{i \in I} x_i^k$$

$$\times \prod_{i \in I} \frac{1 - ax_i^{-1}q^{1-n}}{1 - x_i^{-1}q^{1-|I|}} \prod_{j \notin I} \frac{1 - ax_j}{1 - x_j q^{|I|}} \prod_{i \in I, j \notin I} \frac{x_i - qx_j}{x_i - x_j},$$

where the sum on the left-hand side is over partitions λ satisfying $\lambda_1 \leqslant k$ and $\ell(\lambda) \leqslant n$, $[n] := \{1, \ldots, n\}$, and $|I|$ is the cardinality of the set I.

We postpone the proof of this result to the next subsection, but we give the following usefull consequence.

Corollary 16. *For positive integers n, k, and for any complex numbers a, z, we have*

$$(24) \quad \sum_{\lambda \subseteq (k^n)} z^{|\lambda|} q^{2n(\lambda)} \frac{(a;q^{-1})_{\ell(\lambda)}(a;q^{-1})_{n-m_k(\lambda)}(q)_n}{(q)_{n-\ell(\lambda)} b_\lambda(q)} = \sum_{r=0}^{n} (-1)^r z^{(k+1)r} q^{(2k+3)\binom{r}{2}}$$

$$\times (1 - zq^{2r-1}) \frac{(q^{n-r+1})_r (azq^r)_{n-r}(a;q^{-1})_r(aq^{1-n}/z;q^{-1})_r(a;q^{-1})_{n-r}}{(q)_r(zq^{r-1})_{n+1}}.$$

Proof. We consider the specialization $x_i = zq^{i-1}$ in (23). In that case note that for any $I \subseteq [n]$,

$$\prod_{i \in I, j \notin I} \frac{1 - qx_i^{-1}x_j}{1 - x_i^{-1}x_j} \neq 0 \iff \exists r \in \{0, \cdots, n\} \mid I = \{1, \ldots, r\}.$$

Thus, by using (2), we get the desired result after a few manipulations on the right-hand side. $\square$

Note that when $n \to \infty$, identity (24) reduces to Stembridge's Theorem 3.4 (b) with $b = 0$ in [Ste90]. Moreover, when $a = 0$, (24) corresponds to Warnaar's identity (6.10) from [War06], which is itself equivalent to Stembridge's Theorem 1.3 (b) from [Ste90]. Now we can easily see that (24) contains (22) (but unfortunately not (21)) as a consequence. Indeed, on the left-hand side of (24), replace λ by μ, k by ℓ, and take $a = zq^n$ to get

$$\sum_{\mu_1 \leqslant \ell} z^{|\mu|} q^{2n(\mu)} \frac{(zq^n;q^{-1})_{l(\mu)}(zq^n;q^{-1})_{n-\mu'_\ell}(q)_n}{(q)_{n-l(\mu)} b_\mu(q)} = \sum_{r=0}^{n} (-1)^r z^{(\ell+1)r} q^{(2\ell+3)\binom{r}{2}}$$

$$\times (1 - zq^{2r-1}) \frac{(q^{n-r+1})_r (z^2 q^{r+n})_{n-r}(zq^n;q^{-1})_r(q;q^{-1})_r(zq^n;q^{-1})_{n-r}}{(q)_r(zq^{r-1})_{n+1}}.$$

Note that on the right-hand side, $(q;q^{-1})_r = 0$ unless $r = 0$ or 1, therefore letting finally $n \to \infty$ yields (22).

7.2. Proof of the finite form of the q-binomial theorem for Hall-Littlewood polynomials.
Consider the generating function

$$S(u) = \sum_{\lambda_0, \lambda} q^{n(\lambda)} c_{\lambda_0}(\lambda, a) P_\lambda(x;q) u^{\lambda_0},$$

where the sum is over all partitions $\lambda = (\lambda_1, \ldots, \lambda_n)$ and the integers $\lambda_0 \geqslant \lambda_1$, and

$$c_k(\lambda, a) = (a;q^{-1})_{l(\lambda)}(a;q^{-1})_{n-m_k(\lambda)}.$$

Assume $\lambda = (\mu_1^{r_1} \mu_2^{r_2} \ldots \mu_k^{r_k})$, where $\mu_1 > \mu_2 > \cdots > \mu_k \geqslant 0$ and $(r_1, \ldots, r_k)$ is a composition of n. Let S_n^λ be the set of permutations of S_n which fix λ. Each $w \in S_n/S_n^\lambda$ corresponds to a surjective mapping $f : x \longrightarrow \{1, 2, \ldots, k\}$ such that $|f^{-1}(i)| = r_i$. For any subset y of $x = \{x_1, \ldots, x_n\}$, let $p(y)$ denote the product of the elements of y (in particular, $p(\emptyset) = 1$). We can rewrite Hall-Littlewood functions as follows

$$P_\lambda(x; q) = \sum_f p(f^{-1}(1))^{\mu_1} \cdots p(f^{-1}(k))^{\mu_k} \prod_{f(x_i) < f(x_j)} \frac{x_i - q x_j}{x_i - x_j},$$

summed over all surjective mappings $f : x \longrightarrow \{1, 2, \ldots, k\}$ such that $|f^{-1}(i)| = r_i$. Furthermore, each such f determines a *filtration* of x

$$(25) \qquad \mathcal{F} : \quad \emptyset = F_0 \subsetneq F_1 \subsetneq \cdots \subsetneq F_k = x,$$

according to the rule $x_i \in F_l \iff f(x_i) \leqslant l$ for $1 \leqslant l \leqslant k$. Conversely, such a filtration $\mathcal{F} = (F_0, F_1, \ldots, F_k)$ determines a surjection $f : x \longrightarrow \{1, 2, \ldots, k\}$ uniquely. Thus we can write

$$(26) \qquad P_\lambda(x; q) = \sum_{\mathcal{F}} \pi_{\mathcal{F}} \prod_{1 \leqslant i \leqslant k} p(F_i \setminus F_{i-1})^{\mu_i},$$

summed over all the filtrations $\mathcal{F}$ such that $|F_i| = r_1 + r_2 + \cdots + r_i$ for $1 \leqslant i \leqslant k$, and

$$\pi_{\mathcal{F}} := \prod_{f(x_i) < f(x_j)} \frac{x_i - q x_j}{x_i - x_j},$$

where f is the function defined by $\mathcal{F}$. Now let $\nu_i = \mu_i - \mu_{i+1}$ if $1 \leqslant i \leqslant k-1$ and $\nu_k = \mu_k$, thus $\nu_i > 0$ if $i < k$ and $\nu_k \geqslant 0$. Furthermore, let $\mu_0 = \lambda_0$ and $\nu_0 = \mu_0 - \mu_1$ in the definition of $S(u)$, so that $\nu_0 \geqslant 0$ and $\mu_0 = \nu_0 + \nu_1 + \cdots + \nu_k$. Since the lengthes of the columns of λ are $|F_j| = r_1 + \cdots + r_j$ with multiplicities ν_j for $1 \leqslant j \leqslant k$, we have

$$n(\lambda) = \sum_{i=1}^k \nu_i \binom{|F_i|}{2},$$

$$\ell(\lambda) = n\chi(\nu_k \neq 0) + |F_{k-1}|\chi(\nu_k = 0),$$

$$m_k(\lambda) = \chi(\nu_0 \neq 0) + |F_1|\chi(\nu_0 = 0),$$

and

$$c_{\lambda_0}(\lambda, a) = (a; q^{-1})_n \left(\chi(\nu_k \neq 0) + \frac{(a; q^{-1})_{|F_{k-1}|}}{(a; q^{-1})_n} \chi(\nu_k = 0) \right)$$

$$\times \left(\chi(\nu_0 \neq 0) + \frac{(a; q^{-1})_{n-|F_1|}}{(a; q^{-1})_n} \chi(\nu_0 = 0) \right).$$

For any filtration $\mathcal{F}$ of x define

$$\mathcal{A}_{\mathcal{F}}(x, a, u) := (a; q^{-1})_n$$
$$\times \prod_{j=0}^k \left(\frac{q^{\binom{|F_j|}{2}} p(F_j) u}{1 - q^{\binom{|F_j|}{2}} p(F_j) u} + \frac{(a; q^{-1})_{|F_{k-1}|}}{(a; q^{-1})_n} \chi(F_j = x) + \frac{(a; q^{-1})_{n-|F_1|}}{(a; q^{-1})_n} \chi(F_j = \emptyset) \right).$$

Letting $F(x)$ be the set of filtrations of x, we get $S(u) = \sum_{\mathcal{F} \in F(x)} \pi_{\mathcal{F}} \mathcal{A}_{\mathcal{F}}(x, a, u)$.

Hence $S(u)$ is a rational function of u with simple poles at $1/p(y)q^{\binom{|y|}{2}}$, where y is a subset of x. We are now proceeding to compute the corresponding residue $c(y)$

at each pole $u = 1/p(y)q^{\binom{|y|}{2}}$. Let us start with $c(\emptyset)$. Writing $\lambda_0 = \lambda_1 + k$ with $k \geqslant 0$, we see that

$$
\begin{aligned}
S(u) &= \sum_\lambda q^{n(\lambda)}(a; q^{-1})_{l(\lambda)} P_\lambda(x; q) u^{\lambda_1} \sum_{k \geqslant 0} u^k \frac{(a; q^{-1})_{n-m_{\lambda_1+k}}}{(a; q^{-1})_n} \\
&= \sum_\lambda q^{n(\lambda)}(a; q^{-1})_{l(\lambda)} P_\lambda(x; q) u^{\lambda_1} \left(\frac{u}{1-u} + \frac{(a; q^{-1})_{n-m_{\lambda_1}}}{(a; q^{-1})_n} \right).
\end{aligned}
$$

It follows from (3) that

$$
c(\emptyset) = [S(u)(1-u)]_{u=1} = \prod_{i \geqslant 1} \frac{1 - ax_i}{1 - x_i} =: \phi(x; a),
$$

which gives the identity

$$
(27) \qquad \sum_{\mathcal{F} \in F(x)} \pi_\mathcal{F} \mathcal{A}_\mathcal{F}(x, a, u)(1 - u)|_{u=1} = \phi(x; a).
$$

For the computations of other residues, we need some more notations. For any $y \subseteq x$ and any $\alpha \in \mathbb{C}$, let $q^\alpha y = \{q^\alpha x_i, x_i \in y\}$, $y' = x \setminus y$, and $-y = \{x_i^{-1} : x_i \in y\}$. Let $y \subseteq x$, then

$$
(28) \qquad c(y) = \left[\sum_\mathcal{F} \pi_\mathcal{F} \mathcal{A}_\mathcal{F}(x, a, u)(1 - p(y)q^{\binom{|y|}{2}}u) \right]_{u = p(-y)q^{-\binom{|y|}{2}}}.
$$

If $y \notin \mathcal{F}$, the corresponding summand is equal to 0. Thus we need only to consider the following filtrations $\mathcal{F}$

$$
\emptyset = F_0 \subsetneq \cdots \subsetneq F_p = y \subsetneq \cdots \subsetneq F_k = x \qquad 1 \leqslant p \leqslant k.
$$

We may then split $\mathcal{F}$ into two filtrations $\mathcal{F}_1$ and $\mathcal{F}_2$

$$
\begin{aligned}
\mathcal{F}_1 &: \quad \emptyset \subsetneq -q^{-|y|+1}(y \setminus F_{p-1}) \subsetneq \cdots \subsetneq -q^{-|y|+1}(y \setminus F_1) \subsetneq -q^{-|y|+1}y, \\
\mathcal{F}_2 &: \quad \emptyset \subsetneq q^{|y|}(F_{p+1} \setminus y) \subsetneq \cdots \subsetneq q^{|y|}(F_{k-1} \setminus y) \subsetneq q^{|y|}y'.
\end{aligned}
$$

As

$$
(|y| - 1)(|y| - |F_j|) + \binom{|F_j|}{2} - \binom{|y|}{2} = \binom{|y| - |F_j|}{2} \text{ for } |y| \geqslant |F_j|,
$$

$$
|y|(|F_j| - |y|) + \binom{|F_j|}{2} - \binom{|y|}{2} = \binom{|F_j| - |y|}{2} \text{ for } |y| \leqslant |F_j|,
$$

and

$$
\pi_\mathcal{F}(x) = \pi_{\mathcal{F}_1}(-q^{-|y|+1}y)\pi_{\mathcal{F}_2}(q^{|y|}y') \prod_{x_i \in y, x_j \in y'} \frac{1 - qx_i^{-1}x_j}{1 - x_i^{-1}x_j},
$$

we can write, setting $v = p(y)q^{\binom{|y|}{2}}u$, and using (28),

$$
\begin{aligned}
c(y) &= \left[\sum_{\mathcal{F} \in F(x)} \pi_\mathcal{F} \mathcal{A}_\mathcal{F}(x, a, u) \left(1 - p(y)q^{\binom{|y|}{2}}u \right) \right]_{u = p(-y)q^{-\binom{|y|}{2}}} \\
&= \frac{(a; q^{-1})_n}{(aq^{|y|-n}; q^{-1})_{|y|}(aq^{-|y|}; q^{-1})_{n-|y|}} \prod_{x_i \in y, x_j \in y'} \frac{1 - qx_i^{-1}x_j}{1 - x_i^{-1}x_j} \\
&\quad \times \left[\sum_{\mathcal{F}_1} \pi_{\mathcal{F}_1} \mathcal{A}_{\mathcal{F}_1} \left(-q^{-|y|+1}y, aq^{|y|-n}, v \right) (1 - v) \right]_{v=1} \\
&\quad \times \left[\sum_{\mathcal{F}_2} \pi_{\mathcal{F}_2} \mathcal{A}_{\mathcal{F}_2} \left(q^{|y|}y', aq^{-|y|}, v \right) (1 - v) \right]_{v=1}.
\end{aligned}
$$

Then, using (27), we get

$$
\begin{aligned}
c(y) \;=\; & \phi\left(-q^{1-|y|}y; aq^{|y|-n}\right)\, \phi\left(q^{|y|}y'; aq^{-|y|}\right) \\
& \times \frac{(a;q^{-1})_{|y|}(a;q^{-1})_{n-|y|}}{(a;q^{-1})_n} \prod_{x_i\in y, x_j\in y'} \frac{1-qx_i^{-1}x_j}{1-x_i^{-1}x_j}.
\end{aligned}
$$

Encoding each subset y of x by the corresponding subset $I \subseteq [n]$ and extracting the coefficient u^k in

$$
S(u) = \sum_{y\subseteq x} \frac{c(y)}{1-q^{\binom{|y|}{2}}p(y)u},
$$

we get the result.

8. Acknowledgements

References

[ASW99] George E. Andrews, Anne Schilling, and S. Ole Warnaar. An A_2 Bailey Lemma and Rogers-Ramanujan-type Identities. *J. Amer. Math. Soc.*, 12:677–702, 1999.

[Bha05] Manjul Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math. (2)*, 162(2):1031–1063, 2005.

[BS10a] Manjul Bhargava and Arul Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Preprint available on arXiv:1006.1002*, 2010.

[BS10b] Manjul Bhargava and Arul Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Preprint available on arXiv:1007.0052*, 2010.

[But94] Lynne M. Butler. Subgroup lattices and symmetric functions. *Mem. Amer. Math. Soc.*, 112:no. 539, vi+160 pp., 1994.

[CL84] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups. In *Number theory (New York, 1982)*, volume 1052 of *Lecture Notes in Math.*, pages 26–36. Springer, Berlin, 1984.

[CM90] Henri Cohen and Jacques Martinet. Étude heuristique des groupes de classes des corps de nombres. *J. Reine Angew. Math.*, 404:39–76, 1990.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[Del48] S. Delsarte. Fonctions de möbius sur les groupes abeliens finis. *Ann. Math.*, 49:600–609, 1948.

[Del01] Christophe Delaunay. Heuristics on Tate-Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$. *Experiment. Math.*, 10(2):191–196, 2001.

[Del07] Christophe Delaunay. Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics. In *Ranks of elliptic curves and random matrix theory*, volume 341 of *London Math. Soc. Lecture Note Ser.*, pages 323–340. Cambridge Univ. Press, Cambridge, 2007.

[Del11] Christophe Delaunay. Averages of groups involving p^l-rank and combinatorial identities. *Journal of Number Theory*, 131:536–551, 2011.

[DH71] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A*, 322(1551):405–420, 1971.

[FK06] Étienne Fouvry and Jürgen Klüners. Cohen-Lenstra heuristics of quadratic number fields. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 40–55. Springer, Berlin, 2006.

[FK07] Étienne Fouvry and Jürgen Klüners. On the 4-rank of class groups of quadratic number fields. *Invent. Math.*, 167(3):455–513, 2007.

[GR04] George Gasper and Mizan Rahman. *Basic Hypergeometric Series, second edition*, volume 96 of *Encyclopedia of mathematics and its applications*. Cambridge Univ. Press, Cambridge, 2004.

[Hal38] Philip Hall. A partition formula connected with Abelian groups. *Comment. Math. Helv.*, 11(1):126–129, 1938.

[HB93]   D. R. Heath-Brown. The size of Selmer groups for the congruent number problem. *Invent. Math.*, 111(1):171–195, 1993.

[HB94]   D. R. Heath-Brown. The size of Selmer groups for the congruent number problem. II. *Invent. Math.*, 118(2):331–370, 1994. With an appendix by P. Monsky.

[IJZ06] Masao Ishikawa, Frédéric Jouhet, and Jiang Zeng. A generalization of Kawanaka's identity for Hall-Littlewood polynomials and applications. *J. Algebraic Combin.*, 23(4):395–412, 2006.

[JZ05]   Frédéric Jouhet and Jiang Zeng. New identities for Hall-Littlewood polynomials and applications. *Ramanujan J.*, 10(1):89–112, 2005.

[Kan11] Daniel M. Kane. On the Ranks of the 2-Selmer Groups of Twists of a Given Elliptic Curve. *Preprint available on arXiv: 1009.1365*, 2011.

[Kow07] E. Kowalski. Elliptic curves, rank in families and random matrices. In *Ranks of elliptic curves and random matrix theory*, volume 341 of *London Math. Soc. Lecture Note Ser.*, pages 7–52. Cambridge Univ. Press, Cambridge, 2007.

[Las07] Alain Lascoux. Adding 1 to the argument of a Hall-Littlewood polynomial. *Sém. Lothar. Combin.*, 54(Art. B54n):17 pp, 2005/07.

[LRW09] Alain Lascous, Eric Rains, and S. Ole Warnaar. Nonsymmetric interpolation Macdonald polynomials and gl_n basic hypergeometric series. *Transf. Groups*, 14:613–647, 2009.

[LS06]   Michel Lassalle and Michael Schlosser. Inversion of the Pieri formula for Macdonald polynomials. *Adv. Math.*, 202(2):289–325, 2006.

[Mac95] Ian G. Macdonald. *Symmetric Functions and Hall Polynomials, second edition*. Oxford University Press, New-York, 1995.

[Oko97] Andrei Okounkov. Binomial formula for Macdonald polynomials and applications. *Math. Res. Lett.*, 4:533–553, 1997.

[PR12]   Bjorn Poonen and Eric Rains. Random maximal isotropic subspaces and Selmer groups. *J. Amer. Math. Soc.*, 25(1):245–269, 2012.

[Sch07] Michael Schlosser. Macdonald polynomials and multivariable basic hypergeometric series. *Vadim Kuznetsov Memorial Issue on Integrable Systems and Related Topics, SIGMA*, 3(056):30 pp., 2007.

[SD08]   Peter Swinnerton-Dyer. The effect of twisting on the 2-Selmer group. *Math. Proc. Cambridge Philos. Soc.*, 145(3):513–526, 2008.

[Ste90] John R. Stembridge. Hall-Littlewood functions, plane partitions, and the Rogers-Ramanujan identities. *Trans. Amer. Math. Soc.*, 319(2):469–498, 1990.

[War06] S. Ole Warnaar. Hall-Littlewood functions and the A_2 Rogers-Ramanujan identities. *Adv. Math.*, 200:403–434, 2006.

[WZ12]   S. Ole Warnaar and Wadim Zudilin. Dedekin's eta function and Rogers-Ramanujan identities. *Bull. London Math. Soc.*, 44:1–11, 2012.

Université de Franche-Comté, Laboratoire de Mathématiques de Besançon, CNRS UMR UMR 6623, Facultés des Sciences et Techniques, 16 route de Gray, 25030 Besançon, France.

E-mail address: `christophe.delaunay@univ-fcomte.fr`

Université de Lyon, CNRS, Université Lyon 1, Institut Camille Jordan, 43, boulevard du 11 novembre 1918, F-69622 Villeurbanne Cedex, France.

E-mail address: `jouhet@math.univ-lyon1.fr`