ACTA ARITHMETICA
164.3 (2014)

The Cohen–Lenstra heuristics, moments and p^j-ranks of some groups

by

Christophe Delaunay (Besançon) and Frédéric Jouhet (Lyon)

1. Introduction and notation. The Cohen–Lenstra heuristics and their generalizations to Tate–Shafarevich groups are models for formulating conjectures related to class groups of number fields and Tate–Shafarevich groups of elliptic curves varying in some natural families. This article deals with the coherence of the model. More precisely, our aim is to prove that a conjecture provided by the Cohen–Lenstra philosophy implies another such conjecture. This work actually extends and generalizes an earlier one by É. Fouvry and J. Klüners [FK06] which deals with class groups; we will follow their presentation and adapt the main techniques of their proofs.

We will use the following notation. The letter d will denote a fundamental discriminant and $\mathrm{C}\ell(K_d)$ the class group associated to the quadratic number field $K_d = \mathbb{Q}(\sqrt{d})$. The letter p will always denote a prime number. If G is a finite abelian group, the p^j-rank of G is defined by $\mathrm{rk}_{p^j}(G) = \dim_{\mathbb{F}_p} p^{j-1}G/p^jG$. For any real valued function f defined over isomorphism classes of finite abelian groups, we say that $f(\mathrm{C}\ell(K_d))$ has *average value* $c_\pm \in \mathbb{R}$ if

$$\frac{\sum_{0<\pm d<X} f(\mathrm{C}\ell(K_d))}{\sum_{0<\pm d<X} 1} = c_\pm + o(1) \qquad \text{as } X \to \infty.$$

If f is the characteristic function of some property, then $c_\pm$ is called the *probability* of the property (or the *density* of the set of the class groups satisfying it).

The Cohen–Lenstra heuristics allow one to formulate conjectures for the average values of $f(\mathrm{C}\ell(K_d)_{\mathrm{odd}})$ for "reasonable" functions f, where $\mathrm{C}\ell(K_d)_{\mathrm{odd}}$ denotes the odd part of $\mathrm{C}\ell(K_d)$. Concerning the 2-part of class

2010 *Mathematics Subject Classification*: 11R29, 11G05.
Key words and phrases: heuristics à la Cohen–Lenstra, class groups of number fields, Selmer groups and Tate–Shafarevich groups of elliptic curves, p^j-ranks of finite abelian groups.

DOI: 10.4064/aa164-3-3

groups, genus theory enables one to determine the structure of $C\ell(K_d)[2]$. However Gerth [Ger84, Ger87] succeeded in generalizing the Cohen–Lenstra heuristics to the 4-part of class groups, and also obtained conjectures for the average values of $f(C\ell(K_d)^2)$ for reasonable functions f.

In particular, the above heuristics give on the one hand a prediction for the average value of the function $f(p^{k\,\mathrm{rk}_p(C\ell(K_d)^2)})$ for all $k \in \mathbb{N}$, and on the other hand a prediction for the probability that $\mathrm{rk}_p(C\ell(K_d)^2) = r$ for all $r \in \mathbb{N}$ (note that for odd p, $\mathrm{rk}_p(C\ell(K_d)^2) = \mathrm{rk}_p(C\ell(K_d))$). In [FK06], the authors proved that the former prediction implies the latter. The aim of this article is to generalize the results of [FK06] in two directions. First, we will consider higher moments (including for example the average values of $f(p^{k\,\mathrm{rk}_{p^j}(C\ell(K_d)^2)})$ for all positive integers (k, j)) and probability laws of p^j-ranks for $j \geq 1$. Note that our discussion about the class groups remains true if we replace $C\ell(K_d)$ by the narrow class group of K_d (see also [FK07]). Secondly, we will obtain analogous results concerning heuristics on Tate–Shafarevich groups and on Selmer groups of elliptic curves [Del01, Del07, DJ12].

We recall for $(a, q) \in \mathbb{C}^2$ with $|q| < 1$ and $k \in \mathbb{Z}$ the *q-shifted factorial*

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

and $(a;q)_\infty := \lim_{k\to\infty}(a;q)_k$. Note that $(1/p;1/p)_k = \eta_k(p)$, where η_k is the function defined in [CL84] and used in [FK06]. We will also use the *q-binomial coefficient*

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \frac{(q;q)_n}{(q;q)_k(q;q)_{n-k}} \in \mathbb{N}[q].$$

A *partition* $\lambda := (\lambda_1 \geq \lambda_2 \geq \cdots)$ of a nonnegative integer n is a finite decreasing sequence of nonnegative integers whose sum is equal to n. If λ is a partition of n, we write $|\lambda| = n$ and the notation $\lambda = 1^{m_1}2^{m_2}\cdots\ell^{m_\ell}$ means that m_i is the multiplicity of the integer i in λ (hence, we have $n = \lambda_1 + \lambda_2 + \cdots = |\lambda| = m_1 + 2m_2 + \cdots + \ell m_\ell$). If $\mu := (\mu_1 \geq \mu_2 \geq \cdots)$ is a second integer partition, then we define $(\lambda|\mu) := \sum_i \lambda_i\mu_i$ (we will often use the statistics $(\lambda|\lambda) = \sum_i \lambda_i^2$, which must not be mistaken for $|\lambda|^2 = (\sum_i \lambda_i)^2$). Finally, the notation $\mu \subseteq \lambda$ means that $\mu_i \leq \lambda_i$ for all $i \geq 1$.

Recall that a finite abelian p-group G has *type* $\lambda = 1^{m_1}\cdots\ell^{m_\ell}$ if

$$G \simeq (\mathbb{Z}/p\mathbb{Z})^{m_1} \oplus \cdots \oplus (\mathbb{Z}/p^\ell\mathbb{Z})^{m_\ell}.$$

If $\lambda = 1^{m_1}\cdots\ell^{m_\ell}$ is an integer partition, we denote by $\lambda' := (\lambda'_1 \geq \lambda'_2 \geq \cdots)$ its *conjugate* defined by $\lambda'_k = \sum_{j=k}^{\ell} m_j$ for all k. We have $|\lambda| = |\lambda'|$.

As in [DJ12], we denote by $C_{\lambda/\mu}(p)$ the number of subgroups of type μ in a finite abelian p-group of type λ, which can be expressed by

$$C_{\lambda/\mu}(p) = p^{\sum_{i\geq 1}\mu'_{i+1}(\lambda'_i-\mu'_i)}\prod_{i\geq 1}\begin{bmatrix}\lambda'_i-\mu'_{i+1}\\ \lambda'_i-\mu'_i\end{bmatrix}_p, \tag{1.1}$$

showing that it is a polynomial in the variable p, with positive integral coefficients.

In order to simplify the notations and to get a unified result (both for $p=2$ and odd primes), we write $\mathrm{C}(K_d) := \mathrm{C}\ell(K_d)^2$. Note that for $p\geq 3$ and $j\in\mathbb{N}$, the p^j-ranks of $C(K_d)$ and of $\mathrm{C}\ell(K_d)$ are the same.

Using the Cohen–Lenstra philosophy [CL84] and a combinatorial analysis, we obtained the following conjecture [DJ12, Conjecture 1].

Conjecture 1.1. *For any positive integer ℓ, let $\lambda = 1^{m_1}2^{m_2}\cdots\ell^{m_\ell}$ be an integer partition. As d varies over the set of fundamental negative discriminants, the average of $|\mathrm{C}(K_d)[p]|^{m_1}|\mathrm{C}(K_d)[p^2]|^{m_2}\cdots|\mathrm{C}(K_d)[p^\ell]|^{m_\ell}$ is equal to*

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

where the sum is over all integer partitions $\mu\subseteq\lambda$. Similarly, as d varies over the set of fundamental positive discriminants, the average of the product $|\mathrm{C}(K_d)[p]|^{m_1}|\mathrm{C}(K_d)[p^2]|^{m_2}\cdots|\mathrm{C}(K_d)[p^\ell]|^{m_\ell}$ is equal to

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

Concerning the probability laws of the p^j-ranks $\mathrm{rk}_{p^j}(\mathrm{C}(K_d))$, the following conjecture comes naturally from [Del11, Corollary 11].

Conjecture 1.2. *Let ℓ be a positive integer and $\mu := \mu_1\geq\cdots\geq\mu_\ell\geq 0$ a partition of length $\ell(\mu)\leq\ell$ (i.e., $\mu_{\ell+1}=0$). Then, as d varies over the set of fundamental negative discriminants, the probability that $\mathrm{rk}_{p^j}(\mathrm{C}(K_d)) = \mu_j$ for all $1\leq j\leq\ell$ is equal to*

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

Moreover, as d varies over the set of fundamental positive discriminants, the probability that $\mathrm{rk}_{p^j}(\mathrm{C}(K_d)) = \mu_j$ for all $1\leq j\leq\ell$ is equal to

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

Little is known about these conjectures. Davenport and Heilbronn [DH71] proved Conjecture 1.1 for $p=3$ and $\lambda=1^1$. In [FK07], Fouvry and Klüners

proved Conjecture 1.1 for $p = 2$ (both for the class group and the narrow class group of K_d) and any $\lambda = 1^{m_1}$.

The conjectures mentioned in the introduction coming from the seminal work of [CL84] and studied in [FK07, FK06] correspond to Conjecture 1.1 for $\lambda = 1^{m_1}$ and Conjecture 1.2 for $\ell = 1$. More precisely, if $\lambda = 1^m$, Conjecture 1.1 says that the average of $|\mathrm{C}(K_d)[p]|^m$ for imaginary (resp. real) quadratic fields is equal to (in the notations of [DJ12])

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

Those correspond to $\mathcal{N}(n,p)$ (resp. $\mathcal{M}_n(p)$) used in [FK07, FK06]. Fouvry and Klüners proved in [FK06] that if Conjecture 1.1 is true with $\lambda = 1^m$ for all m, then Conjecture 1.2 is true with $\ell = 1$ for all $\mu_1 \geq 0$. We will adapt their proof and use a result in [DJ12] to simplify one of its steps in order to obtain the following generalization.

THEOREM 1.3. *Let ℓ be a positive integer and assume that for any $\lambda = 1^{m_1} 2^{m_2} \cdots \ell^{m_\ell}$, as d varies over the set of fundamental negative discriminants, the average of $|\mathrm{C}(K_d)[p]|^{m_1} |\mathrm{C}(K_d)[p^2]|^{m_2} \cdots |\mathrm{C}(K_d)[p^\ell]|^{m_\ell}$ is equal to $\sum_{\mu \subseteq \lambda} C_{\lambda/\mu}(p)$. Then for any $\mu_1 \geq \cdots \geq \mu_\ell \geq 0$, as d varies over the set of fundamental negative discriminants, the probability that $\mathrm{rk}_{p^j}(\mathrm{C}(K_d)) = \mu_j$ for all $1 \leq j \leq \ell$ is equal to*

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

Finally, assume that for any positive integer ℓ and any $\lambda = 1^{m_1} \cdots \ell^{m_\ell}$, as d varies over the set of fundamental positive discriminants, the average of $|\mathrm{C}(K_d)[p]|^{m_1} |\mathrm{C}(K_d)[p^2]|^{m_2} \cdots |\mathrm{C}(K_d)[p^\ell]|^{m_\ell}$ is $\sum_{\mu \subseteq \lambda} C_{\lambda/\mu}(p) p^{-|\mu|}$. Then for any $\mu_1 \geq \cdots \geq \mu_\ell$, as d varies over the set of fundamental positive discriminants, the probability that $\mathrm{rk}_{p^j}(\mathrm{C}(K_d)) = \mu_j$ for all $1 \leq j \leq \ell$ is equal to

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

One can also adapt the Cohen–Lenstra heuristics to Tate–Shafarevich groups of elliptic curves. If E is an elliptic curve defined over $\mathbb{Q}$, we denote by $Ш(E)$ its Tate–Shafarevich group. In this context, *we assume in this article that $Ш(E)[p^\infty]$ is finite for all elliptic curves $E/\mathbb{Q}$* (which is a classical conjecture). In that case, $Ш(E)[p^\infty]$ is a group of type S, i.e. it is endowed with a bilinear, alternating, nondegenerate pairing $\beta \colon Ш(E)[p^\infty] \times Ш(E)[p^\infty] \to \mathbb{Q}/\mathbb{Z}$ (this notion of type S is different from the previously mentioned groups of type λ, where λ is a partition; there will not be any possible confusion).

Let $\mathcal{F}_u$ be the family of elliptic curves E defined over $\mathbb{Q}$ with rank u, ordered by their conductor, $N(E)$ (note that one can replace in our discussion $\mathbb{Q}$ by any other number field K). If f is a real valued function defined over isomorphism classes of groups of type S (see [Del01, Del07]), then we say that $f(Ш(E))$ has *average value* $c \in \mathbb{R}$ for E varying over $\mathcal{F}_u$ if

$$\sum_{\substack{E\in\mathcal{F}_u\\ N(E)<X}} f(Ш(E)) = (c+o(1)) \sum_{\substack{E\in\mathcal{F}_u\\ N(E)<X}} 1 \quad \text{as } X\to\infty.$$

If f is the characteristic function of some property, we say that c is the *probability* of this property (or the *density* of the set of Tate–Shafarevich groups satisfying it) for E varying over $\mathcal{F}_u$. We raised the following conjecture in [DJ12].

Conjecture 1.4. *Let ℓ be a positive integer, let $\lambda = 1^{m_1}2^{m_2}\cdots\ell^{m_\ell}$ be a partition and let u be a nonnegative integer. As $E/\mathbb{Q}$, ordered by conductors, varies over $\mathcal{F}_u$, the average of $|Ш(E)[p]|^{m_1}|Ш(E)[p^2]|^{m_2}\cdots|Ш(E)[p^\ell]|^{m_\ell}$ is equal to*

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

Concerning the probability laws of the p^j-ranks $\mathrm{rk}_{p^j}(Ш(E))$, we have the following [Del11]:

Conjecture 1.5. *Let ℓ be a positive integer, let $\mu = \mu_1 \geq \cdots \geq \mu_\ell \geq 0$ be an integer partition of length $\ell(\mu) \leq \ell$ and let u be a nonnegative integer. As $E/\mathbb{Q}$, ordered by conductors, varies over $\mathcal{F}_u$, the probability that $\mathrm{rk}_{p^j}(Ш(E)) = 2\mu_j$ for all $1 \leq j \leq \ell$ is equal to*

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

As previously, very little is known about these conjectures. Bhargava and Shankar [BS10b, BS10a] obtained several results about the average of $|S(E)_p|$ over all elliptic curves $E/\mathbb{Q}$, where $S(E)_p$ is the p-Selmer group of $E/\mathbb{Q}$. Their results, together with a strong form of the rank conjecture (asserting that the rank of E is 0 or 1 with probability 1/2 each and that elliptic curves with rank ≥ 2 do not contribute to the averages), imply Conjecture 1.4 for $\lambda = 1^1$ and $p = 2, 3$. Heath-Brown [HB93, HB94], then Swinnerton-Dyer [SD08] and Kane [Kan11] also obtained results about $S(E)_2$ when E varies over some families of quadratic twists. Their results, together with a strong rank conjecture, imply Conjecture 1.4 for $\lambda = 1^1$ and $p = 2$ for some families of quadratic twists. Furthermore, Conjecture 1.4 is compatible with the conjecture of Poonen and Rains [PR12].

In the context of elliptic curves, we will prove the following result.

THEOREM 1.6. *Let u be a nonnegative integer and let ℓ be a positive integer. Assume that for any $\lambda = 1^{m_1}2^{m_2}\cdots\ell^{m_\ell}$, as $E/\mathbb{Q}$, ordered by conductors, varies over $\mathcal{F}_u$, the average of $|Ш(E)[p]|^{m_1}|Ш(E)[p^2]|^{m_2}\cdots|Ш(E)[p^\ell]|^{m_\ell}$ is equal to $\sum_{\mu\subseteq\lambda} C_{\lambda/\mu}(p^2)p^{-|\mu|(2u-1)}$. Then for any $\mu_1 \geq \cdots \geq \mu_\ell$, as $E/\mathbb{Q}$ varies over $\mathcal{F}_u$, the probability that $\mathrm{rk}_{p^j}(Ш(E)) = 2\mu_j$ for all $1 \leq j \leq \ell$ is equal to*

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

REMARKS. 1. In Theorem 1.3 (resp. Theorem 1.6) one can replace class groups (resp. Tate–Shafarevich groups) by finite abelian groups (resp. groups of type S) varying in some families. In particular, we can obtain similar results for Selmer groups of elliptic curves (see Section 5).

2. From the laws of the p^j-ranks for all $j = 1,\dots,\ell$ as in Theorems 1.3 and 1.6, one can also deduce the probability that the p^ℓ-rank is equal to some fixed value for a single ℓ. In this case, we recover the results and conjectures from [Coh85] and [Del11].

3. One can also ask if it is possible to deduce the moments from the probability laws of the p^j-ranks for all $j = 1,\dots,\ell$. For this, it seems that we need to know an error term for the probability laws and this error term is not given by the heuristic philosophy. However, the theoretical results of [FK07, HB93, SD08, Kan11] concern the p^j-ranks of the groups studied (with an explicit error term), from which the moments can be deduced.

2. An auxiliary analytic tool. In this section, we prove a generalization of [FK06, Lemma 6] which will be useful later.

LEMMA 2.1. *Let $a \in \mathbb{C}$ with $|a| > 1$ and $g(z) = \sum_{r\geq 0} w_r z^r$ be an entire function with the following properties:*

- *there exists an absolute constant $C > 0$ and $\alpha \in \mathbb{R}$ such that for all $r \in \mathbb{N}$, we have $|w_r| \leq Ca^{-r^2/2+\alpha r}$;*
- *$g(a^m) = 0$ for all $m \in \mathbb{N}$.*

We denote by $\omega \in \mathbb{N}\cup\{\infty\}$ the vanishing order of g at $z = 0$. Then, if $\omega > \alpha - 1/2$, we have $g \equiv 0$ (i.e. $\omega = \infty$).

Proof. Let k be a nonnegative integer. For $|z| = |a|^k$, a direct computation shows that $|g(z)| \leq C'|a|^{(k+\alpha)^2/2}$, where $C' = C\sum_{r\in\mathbb{Z}}|a|^{-(r-\alpha)^2/2}$. Assume that $g \not\equiv 0$. Then [FK06, Lemma 6] gives

$$\sup_{|z|=|a|^k}|g(z)| \gg |a|^{k(k+1)/2+k\omega}.$$

Hence, we must have $(k+\alpha)^2 \geq k(k+1)+2k\omega$ for all $k \in \mathbb{N}$, which implies $\omega \leq \alpha - 1/2$. ∎

COROLLARY 2.2. *Let $\ell \in \mathbb{N}^*$, let $a \in \mathbb{C}$ with $|a| > 1$ and let $g(\underline{z}) = \sum_r w_r z_1^{r_1} \cdots z_\ell^{r_\ell}$ with $\underline{z} = (z_1, \dots, z_\ell) \in \mathbb{C}^\ell$ and where the sum is over all integer partitions $r = r_1 \geq \cdots \geq r_\ell \geq 0$. Assume that:*

- *$|w_r| \leq C a^{-(r|r)/2+\alpha|r|}$ for some absolute constant C and $\alpha < 3/2$;*
- *$g(a^{m_1}, \dots, a^{m_\ell}) = 0$ for all nonnegative integers $m_1, \dots, m_\ell$.*

If $\alpha < 1/2$, then $g \equiv 0$ and $w_r = 0$ for all r. If $\alpha \in [1/2, 3/2[$ and $w_{0,\dots,0} = 0$, then $g \equiv 0$ (therefore $w_r = 0$ for all r).

Proof. If $\ell = 1$, this is proved by the above lemma, since $\omega > \alpha - 1/2$ in both cases under consideration. If $\ell \geq 2$, we fix $(m_2, \dots, m_\ell) \in \mathbb{N}^{\ell-1}$ and set

$$f(z) = \sum_{r_1} z^{r_1} \Big(\sum_{r_1 \geq r_2 \geq \cdots \geq r_\ell} w_{r_1, r_2, \dots, r_\ell} a^{r_2 m_2} \cdots a^{r_\ell m_\ell} \Big).$$

Then $f(z)$ satisfies the condition of the previous lemma since

$$\Big| \sum_{r_2 \geq \cdots \geq r_\ell \geq 0} w_{r_1, r_2, \dots, r_\ell} a^{r_2 m_2} \cdots a^{r_\ell m_\ell} \Big| \ll_{m_2, \dots, m_\ell} a^{-(r_1|r_1)/2+\alpha r_1}.$$

With the conditions of the corollary, we deduce that $f(z) = 0$, therefore for any fixed $r_1 \geq 0$, we must have

$$\sum_{r_1 \geq r_2 \geq \cdots \geq r_\ell \geq 0} w_{r_1, r_2, \dots, r_\ell} a^{r_2 m_2} \cdots a^{r_\ell m_\ell} = 0$$

for all $m_2, \dots, m_\ell$. We conclude by using the fact that when r_1 is fixed,

$$\sum_{r_1 \geq r_2 \geq \cdots \geq r_\ell \geq 0} w_{r_1, r_2, \dots, r_\ell} z_2^{r_2} \cdots z_r^{r_\ell}$$

is a polynomial. ∎

3. Class groups of number fields. We will actually prove a more general result, displayed in Theorem 3.1 below (which clearly implies Theorem 1.3). If K is a number field, we denote by $\mathrm{C}\ell(K)$ its class group. Let $\mathcal{K}$ be a fixed set of number fields ordered by the absolute value of their discriminant $\mathrm{disc}(K)$. If f is a real valued function defined over isomorphism classes of finite abelian groups, then, as before, we say that $f(\mathrm{C}\ell(K))$ has average value $c \in \mathbb{R}$ for K varying over $\mathcal{K}$ if

$$\sum_{\substack{K \in \mathcal{K} \\ |\mathrm{disc}(K)| < X}} f(\mathrm{C}\ell(K)) = (c + o(1)) \sum_{\substack{K \in \mathcal{K} \\ |\mathrm{disc}(K)| < X}} 1 \quad \text{as } X \to \infty.$$

As before, if f is the characteristic function of some property, we say that c is the probability of this property (or the density of the set of the class groups satisfying it) for K varying in $\mathcal{K}$.

THEOREM 3.1. *Let u be a nonnegative integer and let ℓ be a positive integer. Assume that for every integer partition $\lambda = 1^{m_1} 2^{m_2} \cdots \ell^{m_\ell}$, as*

K varies over $\mathcal{K}$, the average of $|\mathrm{C}\ell(K)[p]|^{m_1}\cdots|\mathrm{C}\ell(K)[p^\ell]|^{m_\ell}$ is equal to $\sum_{\mu\subseteq\lambda} C_{\lambda/\mu}(p)p^{-u|\mu|}$. Then for any $\mu_1\geq\cdots\geq\mu_\ell$, as K varies over $\mathcal{K}$, the probability that $\mathrm{rk}_{p^j}(\mathrm{C}\ell(K))=\mu_j$ for all $1\leq j\leq\ell$ is equal to

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

We generalize the proof from [FK06]. First, we will need the following proposition.

PROPOSITION 3.2. *Let $u\in\mathbb{N}$ and $\ell\in\mathbb{N}$. For all $\lambda=1^{m_1}2^{m_2}\cdots\ell^{m_\ell}$ we have*

$$\sum_{\mu\subseteq\lambda} C_{\lambda/\mu}(p)p^{-u|\mu|}=O_{p,\ell}(p^{(\lambda'|\lambda')/2}). \tag{3.1}$$

Proof. Set $C_\lambda:=\sum_{\mu\subseteq\lambda}C_{\lambda/\mu}(p)p^{-u|\mu|}$. The equality

$$\begin{bmatrix}n\\k\end{bmatrix}_p=\frac{(p;p)_n}{(p;p)_k(p;p)_{n-k}}=p^{k(n-k)}\frac{(1/p;1/p)_n}{(1/p;1/p)_k(1/p;1/p)_{n-k}},$$

and $(1/p;1/p)_\infty\leq(1/p;1/p)_k\leq 1$, together with the expression (1.1) of the coefficients $C_{\lambda/\mu}(p)$, imply that

$$C_\lambda\leq C\sum_{\mu\subseteq\lambda}p^{\sum_i\mu_i'(\lambda_i'-\mu_i')}\leq Cp^{\sum_i\lambda_i'^2/4}\sum_{\mu\subseteq\lambda}1$$

for some constant C depending only on p and ℓ (we used $\mu_i'(\lambda_i'-\mu_i')\leq\lambda_i'^2/4$ for all $0\leq\mu_i'\leq\lambda_i'$, noting that $\mu\subseteq\lambda$ if and only if $\mu'\subseteq\lambda'$). Now, since ℓ is fixed, the number of subpartitions $\mu\subseteq\lambda$ is certainly bounded by the product $(\lambda_1+1)(\lambda_2+1)\cdots(\lambda_\ell+1)$. By the arithmetico-geometric mean inequality, we obtain

$$\sum_{\mu\subseteq\lambda}1\leq\left(1+\frac{|\lambda|}{\ell}\right)^\ell=O_\ell(|\lambda|^\ell).$$

Finally, we have $C_\lambda=O_{p,\ell}(p^{(\lambda'|\lambda')/4}|\lambda|^\ell)=O_{p,\ell}(p^{(\lambda'|\lambda')/2})$. ∎

REMARK. As can be seen in the proof of the above proposition, we have the more precise upper bound $C_\lambda=O_{p,\ell}(p^{(\lambda'|\lambda')/4}|\lambda|^\ell)$. Nevertheless, the upper bound given in the proposition will be sufficient for our application.

Proof of Theorem 3.1. For $X\geq 1$ and $r:=r_1\geq\cdots\geq r_\ell\geq 0$, set

$$N(X):=|\{K\in\mathcal{K}\colon|\mathrm{disc}(K)|\leq X\}|,$$
$$N(X,r):=|\{K\in\mathcal{K}\colon|\mathrm{disc}(K)|\leq X,\ \mathrm{rk}_{p^i}(\mathrm{C}\ell(K))=r_i\text{ for all }i=1,\dots,\ell\}|.$$

For every $\lambda = 1^{m_1}2^{m_2}\cdots\ell^{m_\ell}$, Theorem 3.1 implies that

(3.2)
$$\sum_r \frac{N(X,r)}{N(X)} p^{m_1r_1+m_2(r_1+r_2)+\cdots+m_\ell(r_1+\cdots+r_\ell)} = \sum_{\mu\subseteq\lambda} C_{\lambda/\mu}(p)p^{-|\mu|u} + o_\lambda(1),$$

where the sum on the left is over all integer partitions $r = r_1 \geq \cdots \geq r_\ell \geq 0$. Note that $m_1r_1 + m_2(r_1 + r_2) + \cdots + m_\ell(r_1 + \cdots + r_\ell) = (\lambda'|r)$. Hence, equation (3.2) can be written as

$$\sum_r \frac{N(X,r)}{N(X)} p^{(\lambda'|r)} = \sum_{\mu\subseteq\lambda} C_{\lambda/\mu}(p)p^{-|\mu|u} + o_\lambda(1) \quad (X\to\infty). \tag{3.3}$$

For each integer partition r, the sequence $n \mapsto N(n,r)/N(n)$ is a real sequence in the compact set $[0,1]$. We deduce that there exists a real number $d_r \in [0,1]$ and an infinite subset $\mathcal{M}$ of $\mathbb{N}$ such that

$$N(m,r)/N(m) \to d_r \quad (m\in\mathcal{M},\ m\to\infty).$$

Replacing m_i by $2m_i + 1$, we see from (3.2) and Proposition 3.2 that

$$\frac{N(X,r)}{N(X)} \ll_\lambda p^{-(2m_1+1)r_1-(2m_2+1)(r_1+r_2)-\cdots-(2m_\ell+1)(r_1+\cdots+r_\ell)}, \tag{3.4}$$

uniformly in X and r, from which we deduce that

$$\sum_r \frac{N(m,r)}{N(m)} p^{(\lambda'|r)} = O_\lambda(1).$$

Hence by Lebesgue's Dominated Convergence Theorem we have

$$\sum_r d_r p^{(\lambda'|r)} = \sum_{\mu\subseteq\lambda} C_{\lambda/\mu}(p)p^{-|\mu|u}.$$

If we consider the infinite multi-dimensional system

$$\sum_r x_r p^{(\lambda'|r)} = \sum_{\mu\subseteq\lambda} C_{\lambda/\mu}(p)p^{-|\mu|u} \quad \text{for all } \lambda = 1^{m_1}2^{m_2}\cdots\ell^{m_\ell}, \tag{$\mathcal{S}$}$$

where the unknowns are $x_r \geq 0$, then $(d_r)_r$ is a solution of ($\mathcal{S}$). We already know that

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

gives a solution $(x_\mu)_\mu$ (see [DJ12, Theorem 14 or the equality just before]). Therefore we need to prove that there exists at most one solution to the system.

Let $(x_r)_r$ be a solution of ($\mathcal{S}$). Since $\lambda \mapsto \lambda'$ is a bijection, the system is equivalent to

$$\sum_r x_r p^{(\lambda|r)} = C_{\lambda'} \quad \text{for all } \lambda,$$

where $C_{\lambda'}(p)=\sum_{\mu\subseteq\lambda'}C_{\lambda'/\mu}(p)p^{-|\mu|u}=O(p^{(\lambda|\lambda)/2})$ by Proposition 3.2. From $x_r\geq 0$, we deduce $x_r=O(p^{-(\lambda|r)+(\lambda|\lambda)/2})$, so when $\lambda=r$, we get

$$0\leq x_r\leq c_0p^{-(r|r)/2}$$

for some absolute constant c_0. Now, if $(x'_r)_r$ is another solution of $(\mathfrak{S})$, then setting $w_r=x_r-x'_r$, we have a function

$$f(\underline{z})=f(z_1,\dots,z_\ell)=\sum_r w_r z_1^{r_1}\cdots z_\ell^{r_\ell} \tag{3.5}$$

satisfying $f(\underline{z})=0$ if $z_1=p^{m_1},\dots,z_\ell=p^{m_\ell}$ for all $m_1,\dots,m_\ell\in\mathbb{N}$, and

$$|w_r|\leq 2c_0p^{-(r|r)/2}.$$

Thus we can apply Corollary 2.2 to conclude that $x_r=x'_r$. So, as $X\to\infty$, the sequence $N(X,r)/N(X)$ has only one limit point, which is $d_r=x_r$. ∎

Corollary 3.3. *Let u be a nonnegative integer and let ℓ be a positive integer. Assume that for every integer partition $\lambda=1^{m_1}2^{m_2}\cdots\ell^{m_\ell}$, as K varies over $\mathcal{K}$, the average of $|\mathrm{C}\ell(K)[p]|^{m_1}|\mathrm{C}\ell(K)[p^2]|^{m_2}\cdots|\mathrm{C}\ell(K)[p^\ell]|^{m_\ell}$ is equal to $\sum_{\mu\subseteq\lambda}C_{\lambda/\mu}(p)p^{-u|\mu|}$. Then for $k\in\mathbb{N}$, as K varies over $\mathcal{K}$, the probability that $\mathrm{rk}_{p^\ell}(\mathrm{C}\ell(K))=k$ is equal to*

$$\frac{(1/p^{u+k+1};1/p)_\infty}{(1/p;1/p)_k p^{\ell k(u+k)}}\,Q_{1/p,\ell,1}\biggl(\frac{1}{p^{2k+u-1}}\biggr),$$

where $Q_{q,\ell,1}(x):=\displaystyle\sum_{n\geq 0}\frac{(-1)^n x^{\ell n}q^{n(n+1)(2\ell+1)/2-n}(1-xq^{2n+1})}{(q;q)_n(xq^{n+1};q)_\infty}$.

The series $Q_{q,\ell,k}(x)$ was defined by Andrews (see [And74]). The formula of the above corollary is the u-probability that the p^ℓ-rank of a finite abelian p-group is equal to k, as obtained in [Coh85] (note that we use the definition of u-averages and u-probabilities of that article).

Proof of Corollary 3.3. We define $N(X)$ and $N(X,r)$ as before. Moreover, set

$$N(X,\ell,k)=|\{K\in\mathcal{K}\colon |\mathrm{disc}(K)|\leq X \text{ and } \mathrm{rk}_{p^\ell}(\mathrm{C}\ell(K))=k\}|.$$

We have

$$\frac{N(X,\ell,k)}{N(X)}=\sum_{\mu_1\geq\cdots\geq\mu_{\ell-1}\geq k}\frac{N(X,\mu)}{N(X)}, \tag{3.6}$$

where the sum is over integer partitions $\mu=\mu_1\geq\cdots\geq\mu_{\ell-1}\geq\mu_\ell=k$. By the assumptions and Theorem 3.1, we have

$$\lim_{X\to\infty}\frac{N(X,\mu)}{N(X)}=\frac{(1/p^{u+\mu_\ell+1};1/p)_\infty}{p^{\mu_1^2+\cdots+\mu_\ell^2+u(\mu_1+\cdots+\mu_\ell)}\prod_{j=1}^{\ell}(1/p;1/p)_{\mu_j-\mu_{j+1}}}.$$

In (3.6) we take the limit as $X \to \infty$ and use Lebesgue's Dominated Convergence Theorem (with (3.4)) to deduce that the probability that $\mathrm{rk}_{p^\ell}(\mathrm{C}\ell(K)) = k$ is equal to

$$\sum_{\mu_1 \ge \cdots \ge \mu_{\ell-1} \ge \mu_\ell = k} \frac{(1/p^{u+\mu_\ell+1};1/p)_\infty}{p^{\mu_1^2+\cdots+\mu_\ell^2+u(\mu_1+\cdots+\mu_\ell)} \prod_{j=1}^{\ell}(1/p;1/p)_{\mu_j-\mu_{j+1}}}$$
$$= \frac{(1/p^{u+k+1};1/p)_\infty}{p^{\ell k(u+k)}(1/p;1/p)_k} \sum_{\mu_1 \ge \cdots \ge \mu_{\ell-1} \ge 0} \frac{(1/p)^{\mu_1^2+\cdots+\mu_{\ell-1}^2+(u+2k)(\mu_1+\cdots+\mu_{\ell-1})}}{\prod_{j=1}^{\ell-1}(1/p;1/p)_{\mu_j-\mu_{j+1}}},$$

the equality being derived by shifting all indices by k. Now, from [Del11, Proposition 13] (or [And74, eq. (2.5)]), the last sum is exactly

$$Q_{1/p,\ell,1}\left(\frac{1}{p^{2k+u-1}}\right),$$

as expected (note that $Q_{q,1,1}(x) = 1$). ∎

4. Tate–Shafarevich groups of elliptic curves. In this section, we prove Theorem 1.6. We follow the previous proof. We just need an upper bound for the coefficients $\sum_{\mu\subseteq\lambda} C_{\lambda/\mu}(p^2)p^{-|\mu|(2u-1)}$, which is given in the following result.

PROPOSITION 4.1. *Let $u \in \mathbb{N}$ and $\ell \in \mathbb{N}^*$. For all $\lambda = 1^{m_1}\cdots\ell^{m_\ell}$, we have*

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

Proof. We have

$$\sum_{\mu\subseteq\lambda} C_{\lambda/\mu}(p^2)p^{-|\mu|(2u-1)} = \sum_{\mu\subseteq\lambda} p^{2(\sum_i \mu'_{i+1}(\lambda'_i-\mu'_i))} \prod_i \begin{bmatrix} \lambda'_i-\mu'_{i+1} \\ \lambda'_i-\mu'_i \end{bmatrix}_{p^2} p^{-|\mu|(2u-1)}$$
$$\le p^{|\lambda|} \sum_{\mu\subseteq\lambda} p^{2(\sum_i \mu'_{i+1}(\lambda'_i-\mu'_i))} \prod_i \begin{bmatrix} \lambda'_i-\mu'_{i+1} \\ \lambda'_i-\mu'_i \end{bmatrix}_{p^2}.$$

Using the same method as in the proof of Proposition 3.2, we obtain

$$\sum_{\mu\subseteq\lambda} C_{\lambda/\mu}(p^2)p^{-|\mu|(2u-1)} = O_{p,\ell}(p^{(\lambda'|\lambda')/2+|\lambda|}|\lambda|^\ell), \tag{4.1}$$

which implies the upper bound given in the proposition. ∎

Proof of Theorem 1.6. For $r := r_1 \ge \cdots \ge r_\ell \ge 0$, we denote by $2r$ the integer partition $2r := 2r_1 \ge \cdots \ge 2r_\ell$. For $X \ge 1$, set

$$N(X) := |\{E \in \mathcal{F}\colon N_E \le X\}|,$$
$$N(X,r) := |\{E \in \mathcal{F}\colon N_E \le X \text{ and } \mathrm{rk}_{p^i}(Ш(E)) = r_i \text{ for all } i = 1,\dots,\ell\}|.$$

Note that since $Ш(E)$ is a group of type S, $\mathrm{rk}_{p^j}(Ш(E))$ must be even. Hence if one of the r_j's is odd, then $N(X,r)=0$ for all X. So, for any $\lambda = 1^{m_1}2^{m_2}\cdots\ell^{m_\ell}$, the assertion of Theorem 1.6 implies that

$$\sum_r \frac{N(X,2r)}{N(X)} p^{(\lambda'|2r)} = \sum_{\mu\subseteq\lambda} C_{\lambda/\mu}(p^2)p^{-|\mu|(2u-1)} + o_\lambda(1), \tag{4.2}$$

where the sum is over all integer partitions $r=r_1\geq\cdots\geq r_\ell$. As before, we will prove that the sequence $N(X,2r)/N(X)$ has only one limit point as $X\to\infty$. We are led to consider the system

$$(\mathcal{T}) \quad \sum_r x_{2r} p^{(\lambda'|2r)} = \sum_{\mu\subseteq\lambda} C_{\lambda/\mu}(p^2)p^{-|\mu|(2u-1)} \quad \text{for all } \lambda = 1^{m_1}2^{m_2}\cdots\ell^{m_\ell},$$

where the unknowns are $x_{2r}\geq 0$. If e_{2r} is a limit point of $N(X,2r)/N(X)$, then $(e_{2r})_r$ is a solution of $(\mathcal{T})$. We already know that

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

yields a solution $(x_{2\mu})_\mu$ (see [DJ12, Remark after Theorem 14]). If $(x_{2r})_r$ is a solution of $(\mathcal{T})$, then

$$\sum_r x_{2r} p^{2(\lambda|r)} = \sum_{\mu\subseteq\lambda} C_{\lambda'/\mu}(p^2)p^{-|\mu|(2u-1)} \quad \text{for all } \lambda,$$

where $\sum_{\mu\subseteq\lambda} C_{\lambda'/\mu}(p^2)p^{-|\mu|(2u-1)} = O(p^{(\lambda|\lambda)})$, from which we deduce

$$x_{2r} \ll p^{(r|r)-2(r|r)} \ll p^{-(r|r)} = (p^2)^{-(r|r)/2}.$$

Therefore Corollary 2.2 with $a=p^2$ gives the unicity. ∎

Corollary 4.2. *Let u be a nonnegative integer and let ℓ be a positive integer. Assume that for any $\lambda = 1^{m_1}2^{m_2}\cdots\ell^{m_\ell}$, as $E/\mathbb{Q}$, ordered by conductors, varies over $\mathcal{F}_u$, the average of $|Ш(E)[p]|^{m_1}|Ш(E)[p^2]|^{m_2}\cdots|Ш(E)[p^\ell]|^{m_\ell}$ is equal to $\sum_{\mu\subseteq\lambda} C_{\lambda/\mu}(p^2)p^{-|\mu|(2u-1)}$. Then for $k\in\mathbb{N}$, as $E/\mathbb{Q}$ varies over $\mathcal{F}_u$, the probability that $\mathrm{rk}_{p^\ell}(Ш(E))=2k$ is equal to*

$$\frac{(1/p^{2u+2k+1};1/p^2)_\infty}{(1/p^2;1p^2)_k p^{\ell k(2u+2k-1)}} Q_{1/p^2,\ell,1}(1/p^{4k+2u-3}).$$

Proof. We proceed as in the proof of Corollary 3.3. ∎

The formula in the above corollary is the u-probability that the p^ℓ-rank of a finite abelian p-group of type S is equal to $2k$, as obtained in [Del11].

5. Selmer groups of elliptic curves. In the proof of Theorem 1.6, it is essential that $Ш(E)$ is a group of type S and $\mathrm{rk}_{p^j}(Ш(E))$ is even, since on the left hand side of (4.2) the sum involves partitions with only even parts μ_j. Nevertheless, one can ask what should be the p^j-rank probability

laws for other families of groups if we assume that their moments are given as in Conjecture 1.4. This question can be naturally asked in particular for Selmer groups of elliptic curves (or more precisely for the p-primary parts of the Selmer groups). If E is an elliptic curve defined over $\mathbb{Q}$, then we denote by $S(E)$ the p-primary part of its Selmer group. It is the inductive limit of the p^n-Selmer group $S(E)_{p^n}$ of E:

$$S(E) = \varinjlim S(E)_{p^n}.$$

We have the exact sequence

$$0 \to E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to S(E) \to Ш(E)[p^\infty] \to 0,$$

which can be seen as the limit of

$$0 \to E(\mathbb{Q})/p^n E(\mathbb{Q}) \to S(E)_{p^n} \to Ш(E)[p^n] \to 0.$$

We assume for simplicity that $E(\mathbb{Q})_{\mathrm{tors}}$ is trivial: this is not a restriction since we are considering averaging over elliptic curves, and on average, elliptic curves have trivial rational torsion. The Selmer group $S(E)$ can be an infinite group, nevertheless its subgroup of p^n-torsion points is finite and we have

$$S(E)[p^n] = S(E)_{p^n}.$$

We define the p^j-rank of $S(E)$ by $\mathrm{rk}_{p^j}(S(E)) = \mathrm{rk}_{p^j}(S(E)[p^j])$. Note that $\mathrm{rk}_{p^j}(S(E)) = \mathrm{rk}_{p^j}(S(E)[p^k])$ for all $k \geq j$.

Since $Ш[p^\infty]$ is finite by assumption, we have $S(E) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{r(E)}$, where $r(E)$ is the rank of the Mordell–Weil group $E(\mathbb{Q})$ and

$$\mathrm{rk}_{p^j}(S(E)) = r(E) \qquad \text{for } p^j \text{ large enough.}$$

Furthermore,

$$\mathrm{rk}_{p^j}(S(E)) \equiv r(E) \pmod 2,$$

so the parities of $\mathrm{rk}_{p^j}(S(E))$ are determined by the parity of $r(E)$.

If ℓ is a positive integer and $\lambda = 1^{m_1}2^{m_2}\cdots\ell^{m_\ell}$ is an integer partition, then

$$|S(E)[p]|^{m_1}|S(E)[p^2]|^{m_2}\cdots|S(E)[p^\ell]|^{m_\ell}$$

is meaningful and we can consider the average value of this function as E varies over a family of elliptic curves. The work of [PR12] suggests that the p-Selmer groups should behave in a "global" way independently of the rank of E (except for the parity of the p-ranks). From [DJ12], we can extract the following conjecture.

Conjecture 5.1. *Let ℓ be a positive integer and let $\lambda = 1^{m_1}2^{m_2}\cdots\ell^{m_\ell}$ be an integer partition. As $E/\mathbb{Q}$, ordered by conductors, varies over all elliptic curves, the average of $|S(E)[p]|^{m_1}|S(E)[p^2]|^{m_2}\cdots|S(E)[p^\ell]|^{m_\ell}$ is*

equal to

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

If $\ell = 1$, this conjecture is originally due to Poonen and Rains [PR12], where they use a completely different model for Selmer groups.

PROPOSITION 5.2. *Let ℓ be a positive integer and let $\delta \in \{0,1\}$. Assume that for any partition $\lambda = 1^{m_1}2^{m_2}\cdots\ell^{m_\ell}$, the average of*

$$|S(E)[p]|^{m_1}|S(E)[p^2]|^{m_2}\cdots|S(E)[p^\ell]|^{m_\ell}$$

is equal to $\sum_{\mu\subseteq\lambda} C_{\lambda/\mu}(p^2)p^{|\mu|}$ as $E/\mathbb{Q}$, ordered by conductors, varies over a family $\mathcal{F}$ of elliptic curves, and assuming that the even (resp. odd) rank elliptic curves in $\mathcal{F}$ contribute in a ratio α (resp. $1-\alpha$). Then, for all $\mu_1 \geq \cdots \geq \mu_\ell$, as $E/\mathbb{Q}$ varies over $\mathcal{F}$, the probability that $\mathrm{rk}_{p^j}(S(E)) = 2\mu_j + \delta$ for all $1 \leq j \leq \ell$ is equal to

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

Proof. For $X \geq 1$ and $r = r_1 \geq \cdots \geq r_\ell \geq 0$, set as before

$$N(X) := |\{E \in \mathcal{F}\colon N_E \leq X\}|,$$
$$N(X,r) := |\{E \in \mathcal{F}\colon N_E \leq X \text{ and } \mathrm{rk}_{p^i}(S(E)) = r_i \text{ for all } i = 1,\dots,\ell\}|.$$

Let $\lambda = 1^{m_1}2^{m_2}\cdots\ell^{m_\ell}$ be an integer partition. Since the $\mathrm{rk}_{p^j}(S(E))$'s all have the same parity for $j \in \mathbb{N}$, and by the assumptions of the proposition, we have

$$\sum_r \frac{N(X,2r)}{N(X)}p^{(\lambda'|2r)} = \alpha\sum_{\mu\subseteq\lambda} C_{\lambda/\mu}(p^2)p^{|\mu|} + o_\lambda(1),$$
$$\sum_r \frac{N(X,2r+1)}{N(X)}p^{(\lambda'|2r+1)} = (1-\alpha)\sum_{\mu\subseteq\lambda} C_{\lambda/\mu}(p^2)p^{|\mu|} + o_\lambda(1).$$

For $\delta \in \{0,1\}$, set

$$e_{2\mu+\delta} = \frac{(1/p^{2\delta+2\mu_\ell+1};1/p^2)_\infty}{p^{2(\mu_1^2+\cdots+\mu_\ell^2)+(2\delta-1)(\mu_1+\cdots+\mu_\ell)}\prod_{j=1}^{\ell}(1/p^2;1/p^2)_{\mu_j-\mu_{j+1}}}. \tag{5.1}$$

Thus for $\delta = 0$, we recover $e_{2\mu}$ which was defined in the previous section, where we already saw that

$$\sum_r \alpha e_{2r}p^{(\lambda'|2r)} = \alpha\sum_{\mu\subseteq\lambda} C_{\lambda/\mu}(p^2)p^{|\mu|},$$

that $(\alpha e_{2r})_r$ is the only solution of the above system, and $N(X,2r)/N(X) \to e_{2r}$ as $X \to \infty$.

Now, by the same arguments as before, there exists a unique solution to the system

$$(\mathcal{T}') \qquad \sum_r (x_{2r+1} p^{(\lambda'|2r+1)}) = (1-\alpha) \sum_{\mu \subseteq \lambda} C_{\lambda/\mu}(p^2) p^{|\mu|} \quad \text{for all } \lambda = 1^{m_1} 2^{m_2} \cdots \ell^{m_\ell},$$

where the unknowns are x_{2r+1}. Furthermore $x_{2r+1} = (1-\alpha)e_{2r+1}$ yields a solution $(x_{2r+1})_r$ of $(\mathcal{T}')$. Indeed, by [DJ12, Remark after Theorem 14],

$$\sum_r e_{2r+1} p^{(\lambda'|2r+1)} = p^{|\lambda'|} \sum_r e_{2r+1} p^{(\lambda'|2r)} = p^{|\lambda|} \sum_{\mu \subseteq \lambda} C_{\lambda/\mu}(p^2) p^{-|\mu|},$$

and moreover by [DJ12, Theorem 1],

$$p^{|\lambda|} \sum_{\mu \subseteq \lambda} C_{\lambda/\mu}(p^2) p^{-|\mu|} = \sum_{\mu \subseteq \lambda} C_{\lambda/\mu}(p^2) p^{|\mu|}.$$

Finally, $N(X, 2r+1)/N(X) \to e_{2r+1}$ as $X \to \infty$. ∎

Now, adapting the proof of Corollary 3.3, we have the following result.

Corollary 5.3. *Let ℓ be a positive integer and let $\delta \in \{0,1\}$. Assume that for every $\lambda = 1^{m_1} 2^{m_2} \cdots \ell^{m_\ell}$ the average of*

$$|S(E)[p]|^{m_1} |S(E)[p^2]|^{m_2} \cdots |S(E)[p^\ell]|^{m_\ell}$$

is equal to $\sum_{\mu \subseteq \lambda} C_{\lambda/\mu}(p^2) p^{|\mu|}$, as $E/\mathbb{Q}$, ordered by conductors, varies over a family $\mathcal{F}$ of elliptic curves, and assuming that the even (resp. odd) rank elliptic curves in $\mathcal{F}$ contribute in a ratio α (resp. $1-\alpha$). Then, for $k \in \mathbb{N}$, the probability that $\mathrm{rk}_{p^\ell}(S(E)) = 2k+\delta$ is equal to

$$(\delta(1-\alpha) + \alpha(1-\delta)) \frac{(1/p^{2k+2\delta+1}; 1/p^2)_\infty}{(1/p^2; 1/p^2)_k p^{\ell k(2k+2\delta-1)}} Q_{1/p^2,\ell,1}(1/p^{4k+2\delta-3}).$$

The value of α can of course be $\neq 1/2$. Furthermore, even in the case of a family of quadratic twists of an elliptic curve E defined over a number field K, it is possible to have $\alpha \neq 1/2$ (see [KMR13a]; in that case we have $K \neq \mathbb{Q}$).

If we consider the family of all elliptic curves, then a general conjecture states that $\alpha = 1/2$, which leads to the following:

Conjecture 5.4. *Let ℓ be a positive integer and let $k \in \mathbb{N}$ and $\delta \in \{0,1\}$. Then, as $E/\mathbb{Q}$, ordered by conductors, varies over all elliptic curves, the probability that $\mathrm{rk}_{p^\ell}(S(E)) = 2k+\delta$ is equal to*

$$f(p, \ell, 2k+\delta) := \frac{1}{2} \frac{(1/p^{2k+2\delta+1}; 1/p^2)_\infty}{(1/p^2; 1/p^2)_k p^{\ell k(2k+2\delta-1)}} Q_{1/p^2,\ell,1}(1/p^{4k+2\delta-3}).$$

For $\ell = 1$, we recover the conjectural distribution X_{Sel_p} of [PR12] and the proved distribution of Sel_2 in [HB93, HB94, Kan11, SD08, KMR13b] for some families of quadratic twists of an elliptic curve.

The conjectural distribution on the p^j-rank of the Selmer groups given above is of course compatible with the rank conjecture. Indeed, note that $Q_{q,\infty,1}(x) = 1/(xq^2;q)_\infty$, from which we easily deduce that

$$\lim_{\ell\to\infty} f(p,\ell,2k+\delta) = \begin{cases} 0 & \text{if } k \geq 1, \\ 1/2 & \text{if } k = 0. \end{cases}$$

Since for ℓ large enough, $\mathrm{rk}_{p^\ell}(S(E)) = r(E)$, we recover the fact that, on average, half of the elliptic curves should have rank 0 and half of the elliptic curves should have rank 1. On the other hand, if we assume Conjecture 5.1 for $\ell = 1$ for infinitely many primes p with $\alpha = 1/2$, then we also recover the previous distribution for the rank of $E(\mathbb{Q})$, since

$$\lim_{p\to\infty} f(p,1,2k+\delta) = \begin{cases} 0 & \text{if } k \geq 1, \\ 1/2 & \text{if } k = 0. \end{cases}$$

We give some numerical approximations for the function $f(p,\ell,2k+\delta)$ for $p = 2, 3, 5$ and for small values of ℓ and of $2k+\delta$ in the following tables.

$p = 2$

$2k+\delta \setminus \ell$	1	2	3
0	0.2097	0.3541	0.4271
1	0.4194	0.4899	0.4987
2	0.2796	0.1456	0.0729
3	0.0798	0.1009	0.0012

$p = 3$

$2k+\delta \setminus \ell$	1	2	3
0	0.3195	0.4398	0.4799
1	0.4792	0.4992	0.4999
2	0.1797	0.0601	0.0201
3	0.0207	0.0007	$2 \cdot 10^{-5}$

$p = 5$

$2k+\delta \setminus \ell$	1	2	3
0	0.3966	0.4793	0.4959
1	0.4958	0.4999	0.4999
2	0.1033	0.0207	0.0041
3	0.0042	$3 \cdot 10^{-5}$	$2 \cdot 10^{-7}$

Remark. As pointed out by the referee, we can also use our techniques for some other situations and in particular the one in the paper [FK10]. There, Fouvry and Klüners studied the class groups and the narrow class groups of quadratic number fields with some restrictions on the discriminants. Set

$$\mathcal{D} = \{d > 0 \text{ fund. disc.} : p \mid d \Rightarrow p \equiv 1 \text{ or } 2 \pmod 4\},$$

and for $X \in \mathbb{R}$, write $\mathcal{D}(X) = \mathcal{D} \cap [1, X]$. Denote by $\mathrm{NC}(K_d)$ the narrow class group of K_d. In [FK10, Theorem 3], the authors proved for all $m \geq 0$

the following result on the moments of the 4-rank of $\mathrm{NC}(K_d)$ (i.e. the 2-rank of $\mathrm{NC}(K_d)^2$):

$$\lim_{X\to\infty} \frac{1}{|\mathcal{D}(X)|} \sum_{d\in\mathcal{D}(X)} 2^{m\,\mathrm{rk}_4(\mathrm{NC}(K_d))} = \prod_{k=0}^{m-1}(1+2^k), \tag{5.2}$$

where the empty product is equal to 1 (moreover, with our notations we have $p=2$, $\ell=1$, and $\lambda=1^m$). They deduced that the probability of having $\mathrm{rk}_4(\mathrm{NC}(K_d)) = r$ is equal to $\alpha_\infty(r) := \prod_{j\geq 1}(1+2^{-j})^{-1}/\prod_{j=1}^{r}(2^j-1)$ ([FK10, Corollary 2]). One can recover the probability law from (5.2) with our results. Indeed, if we look at the equation

$$\sum_{j\geq 0} \tilde{e}_j 2^{mj} = \prod_{k=0}^{m-1}(1+2^k), \tag{5.3}$$

then we set $\tilde{e}_j = 2^{-j}e_j$ (where the e_j's are defined in (5.1), with the raw partition $\mu=(j)$ and $p=2$). Using for $\delta\in\{0,1\}$ the formula

$$\sum_{j\geq 0} e_{2j+\delta} 2^{m(2j+\delta)} = \sum_{\mu\subseteq 1^m} C_{1^m/\mu}(2^2)2^{|\mu|} = \prod_{k=1}^{m}(1+2^k),$$

we deduce that $\tilde{e}_j$ is a solution of (5.3). Hence, the probability of having $\mathrm{rk}_4(\mathrm{NC}(K_d)) = r$ is equal to $2^{-r}e_r$, which is exactly $\alpha_\infty(r)$. The article [FK10] contains other results on (mixed) moments involving narrow class groups and classical class groups. Our study could be used to consider (at least conjecturally) higher and mixed moments with p^j-ranks in more generality. This will be done in a forthcoming publication.

6. Remark on the uniqueness of the solution. In our study relating to Tate–Shafarevich groups, we were led to consider and to discuss the unicity of the solution of the following infinite multi-dimensional system

$$(\mathcal{U}) \quad \sum_r x_r p^{(\lambda|r)} = \sum_{\mu\subseteq\lambda'} C_{\lambda'/\mu}(p^2)p^{-|\mu|(2u-1)} \quad \text{for all } \lambda = 1^{m_1}2^{m_2}\cdots\ell^{m_\ell},$$

where the unknowns are $x_r\geq 0$. We only considered solutions $(x_r)_r$ such that $x_r=0$ if in $r=r_1\geq\cdots\geq r_\ell$ at least one of the r_j's does not have the same parity as r_1. In that case, the term $p^{(\lambda|r)}$ involved in the sum is of the form $p^{(\lambda|2r+\delta)}$, and the factor 2 allowed an asymptotic $0\leq x_{2r+\delta}\ll p^{(-r|r)/2}$ which implied the unicity of the solution. One can ask about the unicity of the solution without the assumption that the partitions involved in the system have parts with the same parity.

Let $\mu\in\mathbb{R}$, and for a partition r define

$$y_r(\mu) = \begin{cases} \mu e_r & \text{if } r \text{ is even,} \\ (1-\mu)e_r & \text{if } r \text{ is odd,} \\ 0 & \text{otherwise.} \end{cases}$$

Then $y_r(\mu)$ is a solution of equation $(\mathcal{U})$. If $x_r \geq 0$ is a solution of $(\mathcal{U})$ then, using (4.1), we see that for any fixed $\alpha > 1$, we have

$$0 \leq x_r \ll p^{-(r|r)/2+\alpha|r|}$$

for all r. Now, if we let $w_r = x_r - y_r(x_{0,\dots,0})$ then it is easy to see that also

$$|w_r| \ll p^{-(r|r)/2+\alpha|r|}$$

(w_r is not necessarily nonnegative), and the function $g(\underline{z}) = \sum_r w_r z_1^{r_1} \cdots z_\ell^{r_\ell}$ satisfies the hypothesis of Corollary 2.2 with $\alpha \in]1, 3/2[$ and with $w_{0,\dots,0} = 0$. Hence $w_r = 0$ for all r and $x_r = y_r(x_{0,\dots,0})$. We deduce the following proposition.

PROPOSITION 6.1. *If $x_r \geq 0$ is a solution of $(\mathcal{U})$ then $x_r = y_r(\mu)$ for some μ. In particular, $x_r = 0$ if r is not an even or odd partition.*

It would be interesting to study the (uniqueness of the) solutions of $(\mathcal{U})$ if we do not assume that $x_r \geq 0$.

Acknowledgments. The authors thank the anonymous referee for his/her comments and remarks.

References

[And74] G. E. Andrews, *An analytic generalization of the Rogers–Ramanujan identities for odd moduli*, Proc. Nat. Acad. Sci. USA 71 (1974), 4082–4085.

[BS10a] M. Bhargava and A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, arXiv:1006.1002 (2010).

[BS10b] M. Bhargava and A. Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank* 0, arXiv:1007.0052 (2010).

[Coh85] H. Cohen, *On the p^k-rank of finite abelian groups and Andrews' generalizations of the Rogers–Ramanujan identities*, Nederl. Akad. Wetensch. Indag. Math. 47 (1985), 377–383.

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

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

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

[Del07] C. 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, London Math. Soc. Lecture Note Ser. 341, Cambridge Univ. Press, Cambridge, 2007, 323–340.

[Del11] C. Delaunay, *Averages of groups involving p^l-rank and combinatorial identities*, J. Number Theory 131 (2011), 536–551.

[DJ12] C. Delaunay and F. Jouhet, *p^ℓ-Torsion points in finite abelian groups and combinatorial identities*, Adv. Math 258 (2014), 13–45.

[FK06] É. Fouvry and J. Klüners, *Cohen–Lenstra heuristics of quadratic number fields*, in: Algorithmic Number Theory, Lecture Notes in Comput. Sci. 4076, Springer, Berlin, 2006, 40–55.

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

[FK10] É. Fouvry and J. Klüners, *On the negative Pell equation*, Ann. of Math. (2) 172 (2010), 2035–2104.

[Ger84] F. Gerth III, *The* 4*-class ranks of quadratic fields*, Invent. Math. 77 (1984), 489–515.

[Ger87] F. Gerth III, *Extension of conjectures of Cohen and Lenstra*, Expo. Math. 5 (1987), 181–184.

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

[HB94] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem. II*, Invent. Math. 118 (1994), 331–370.

[Kan11] D. M. Kane, *On the ranks of the* 2*-Selmer groups of twists of a given elliptic curve*, arXiv:1009.1365 (2011).

[KMR13a] Z. Klagsbrun, B. Mazur, and K. Rubin, *Disparity in Selmer ranks of quadratic twists of elliptic curves*, Ann. of Math. 178 (2013), 287–320.

[KMR13b] Z. Klagsbrun, B. Mazur, and K. Rubin, *A Markov model for Selmer ranks in families of twists*, arXiv:1303.6507 (2013).

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

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

Christophe Delaunay
Université de Franche-Comté
Laboratoire de Mathématiques de Besançon
CNRS UMR 6623
Facultés des Sciences et Techniques
16 route de Gray
25030 Besançon, France
E-mail: christophe.delaunay@univ-fcomte.fr

Frédéric Jouhet
Université de Lyon
CNRS
Université Lyon 1
Institut Camille Jordan
43, boulevard du 11 novembre 1918
F-69622 Villeurbanne Cedex, France
E-mail: jouhet@math.univ-lyon1.fr

Received on 29.5.2013
and in revised form on 28.11.2013 (7463)