Random integral matrices and the Cohen-Lenstra heuristics

Melanie Matchett Wood

American Journal of Mathematics, Volume 141, Number 2, April 2019, pp. 383-398 (Article)

Published by Johns Hopkins University Press
DOI: *https://doi.org/10.1353/ajm.2019.0008*

RANDOM INTEGRAL MATRICES AND THE COHEN-LENSTRA HEURISTICS

By MELANIE MATCHETT WOOD

Abstract. We prove that given any $\epsilon > 0$, random integral $n \times n$ matrices with independent entries that lie in any residue class modulo a prime with probability at most $1 - \epsilon$ have cokernels asymptotically (as $n \to \infty$) distributed as in the distribution on finite abelian groups that Cohen and Lenstra conjecture to be the distribution for class groups of imaginary quadratic fields. This shows the Cohen-Lenstra distribution is universal for finite abelian groups given by generators and random relations—that the distribution of quotients does not depend on the way in which we choose (sufficiently nice) relations. This is a refinement of a result on the distribution of ranks of random matrices with independent entries in $\mathbb{Z}/p\mathbb{Z}$. This is interesting especially in light of the fact that these class groups are naturally cokernels of square matrices. We also prove the analogue for $n \times (n+u)$ matrices.

1. Introduction. The Cohen-Lenstra heuristics are conjectures made by Cohen and Lenstra [CL84] on the distribution of class groups of quadratic number fields. For a prime p, we write G_p for the Sylow p-subgroup of an abelian group G. We write $\mathrm{Cl}(K)$ for the class group of a number field K.

CONJECTURE 1.1. (Cohen and Lenstra [CL84]) *Let S_X^- be the set of negative fundamental discriminants $D \geq -X$. Let p be an odd prime and B be a finite abelian p-group. Then*

$$\lim_{X\to\infty} \frac{\#\left\{ D \in S_X^- \mid \mathrm{Cl}\left(\mathbb{Q}(\sqrt{D})_p\right) \simeq B \right\}}{\left|S_X^-\right|} = \frac{\prod_{k=1}^{\infty}\left(1-p^{-k}\right)}{\left|\mathrm{Aut}(B)\right|}.$$

Friedman and Washington [FW89] show that if $H(n) \in M_{n\times n}(\mathbb{Z}_p)$ is a random matrix drawn with respect to Haar measure on the space of $n \times n$ matrices over the p-adics $\mathbb{Z}_p$, then

$$\lim_{n\to\infty} \mathbb{P}\left(\mathrm{cok}\left(H(n)\right) \simeq B\right) = \frac{\prod_{k=1}^{\infty}\left(1-p^{-k}\right)}{\left|\mathrm{Aut}(B)\right|}. \tag{1}$$

In other words, cokernels of random p-adic square matrices drawn with respect to Haar measure are distributed according to Cohen and Lenstra's conjectured distribution of class groups (asymptotically as the size of the matrices grows).

Manuscript received May 9, 2016; revised September 15, 2017.

Research supported by an American Institute of Mathematics Five-Year Fellowship, a Packard Fellowship for Science and Engineering, a Sloan Research Fellowship, National Science Foundation grants DMS-1301690 and DMS-1652116, and a Vilas Early Career Investigator Award.

American Journal of Mathematics 141 (2019), 383–398.

Let $K = \mathbb{Q}(\sqrt{D})$ for some $D \in S_X^-$, and S be any finite set of primes of K that generate $\mathrm{Cl}(K)$. We write $\mathcal{O}_S^*$ for the S-units in the integers $\mathcal{O}_K$, and I_K^S for the abelian group of fractional ideals generated by the elements of S. Then

$$\mathrm{Cl}(K) = \mathrm{cok}\left(\mathcal{O}_S^* \to I_K^S\right), \tag{2}$$

where the map takes α to the ideal (α). So $\mathrm{Cl}(K)_p = \mathrm{cok}(\mathcal{O}_S^* \otimes_{\mathbb{Z}} \mathbb{Z}_p \to I_K^S \otimes_{\mathbb{Z}} \mathbb{Z}_p)$. Since I_K^S and $\mathrm{im}(\mathcal{O}_S^*) \subset I_K^S$ are both free abelian groups of rank $|S|$, we have written $\mathrm{Cl}(K)_p$ as a cokernel of a p-adic square matrix $R_D \in M_{n\times n}(\mathbb{Z}_p)$. If we choose a random D uniformly in S_X^-, we have a random p-adic square matrix $R_D \in M_{n\times n}(\mathbb{Z}_p)$ (where n depends on D) and Conjecture 1.1 is a statement about the distribution of the cokernels of the random matrices R_D as $X \to \infty$. This perspective on the class group as a cokernel of a random matrix is due to Venkatesh and Ellenberg [VE10, Section 4.1].

One might thus imagine that there could be some sense in which the R_D become equidistributed with respect to Haar measure, and that this would imply Conjecture 1.1. However, in this paper we show that in fact having cokernels distributed according to Cohen and Lenstra's conjectured distribution of class groups is a rather robust feature of random matrix regimes, and so much weaker statements (than Haar equidistribution) about the distribution R_D would also imply Conjecture 1.1.

As a particular example, if $q \in (0,1)$ is any real number, p is a prime, and random matrices $M(n) \in M_{n\times n}(\mathbb{Z}_p)$ have random entries that are independent and are 0 with probability q and 1 with probability $1-q$, then Equation (1) holds with $H(n)$ replaced by $M(n)$. These $M(n)$, with their entries concentrated in $\{0,1\}$, are nowhere near Haar equidistributed in any $\mathbb{Z}_p$, yet they still have the same cokernel distributions as Haar equidistributed random matrices. More generally, we have the following.

THEOREM 1.2. *Let p be a prime and $\epsilon > 0$ a real number, and for each positive integer n, let $M(n)$ be a random matrix valued in $M_{n\times n}(\mathbb{Z}_p)$ with independent entries. Further, for any entry $M(n)_{i,j}$ of any $M(n)$ and any $r \in \mathbb{Z}/p\mathbb{Z}$, we require that $\mathbb{P}(M(n)_{i,j} \equiv r \pmod p) \le 1-\epsilon$. Then for any finite abelian p-group B,*

$$\lim_{n\to\infty} \mathbb{P}(\mathrm{cok}(M(n)) \simeq B) = \frac{\prod_{k=1}^{\infty}(1-p^{-k})}{|\mathrm{Aut}(B)|}.$$

Note that the matrix entries are not required to be identically distributed and can vary with n. Of course, some condition that the matrix entries are not too concentrated, like $\mathbb{P}((M(n))_{i,j} \equiv r \pmod p) \le 1-\epsilon$, is certainly necessary, since if the matrices had even two rows whose values were all $r \pmod p$, then $\mathrm{cok}(M(n))$ could never be the trivial group.

In fact, in Corollary 3.4, we prove a statement about random integral matrices that implies Theorem 1.2, determining not only the Sylow p-subgroups of their

cokernels for a single p, but rather the Sylow p-subgroups of their cokernels simultaneously for any finite set of primes p. We see that the Sylow p-subgroups for different primes p are independent, which agrees with the prediction of Cohen and Lenstra [CL84] for class groups.

The cokernel of an $n \times n$ matrix over $\mathbb{Z}_p$ is the quotient of the free abelian pro-p group on n generators modulo the n relations given by the columns of the matrix. In this light, Theorem 1.2 is a universality result for random abelian p-groups, as it says we get the same universal limiting distribution on cokernels almost no matter how we choose independent relations with independent coefficients to define our group. The universality here is analogous to that in the Central Limit Theorem, which tells us that asymptotic averages of i.i.d. random variables have a Gaussian distribution as their limiting distribution.

Of course, the independence of the matrix entries in Theorem 1.2 is a significant hypothesis (and not true in such a form for class groups), and one might wonder to what extent it is necessary. In [Woo14], it is shown that if one takes the matrices $M(n)$ to be symmetric, but with otherwise independent entries, their cokernels have a *different* distribution than that in Theorem 1.2. The work in that paper was to determine the distribution of Jacobians (a.k.a. sandpile groups) of random graphs, which are a more accessible analogue of class groups. That application also required dealing with the fact that each diagonal entry of the relevant matrix (the graph Laplacian) is dependent on all the entries in its column, and this "small" dependence of the diagonal did not have an effect on the cokernel distribution.

In fact, Cohen and Lenstra [CL84] also make conjectures about class groups of real quadratic (and other totally real abelian) number fields. In particular, if S_X^+ is the set of positive fundamental discriminants $D \leq X$, they conjecture that for every odd prime p and every finite abelian p-group B, we have

$$\lim_{X\to\infty} \frac{\#\{D \in S_X^+ \mid \mathrm{Cl}\big(\mathbb{Q}(\sqrt{D})_p\big) \simeq B\}}{\big|S_X^+\big|} = \frac{\prod_{k=1}^{\infty}\big(1-p^{-k-1}\big)}{|B|\big|\operatorname{Aut}(B)\big|}.$$

We see from equation (2) that these class groups are cokernels of $n \times (n+1)$ matrices, since $\mathcal{O}_S^*$ will have rank $|S|+1$ when the number field K is real quadratic. We in fact prove the following, which follows from Corollary 3.4.

THEOREM 1.3. *Let u be a non-negative integer. For every positive integer n, let $M(n)$ be a random matrix valued in $M_{n\times(n+u)}(\mathbb{Z}_p)$ with entries as in Theorem 1.2. Then,*

$$\lim_{n\to\infty} \mathbb{P}\big(\operatorname{cok}\big(M(n)\big) \simeq B\big) = \frac{\prod_{k=1}^{\infty}\big(1-p^{-k-u}\big)}{|B|^u\big|\operatorname{Aut}(B)\big|}.$$

These distributions on finite abelian groups for other u also arise in the general theory Cohen and Lenstra build to formulate their conjectures.

While the results of this paper are particularly notable for their connection to the Cohen-Lenstra heuristics, the proofs in this paper and the history of previous work lie in the fields of additive combinatorics and probability. If $M(n) \in M_{n\times n}(\mathbb{Z}_p)$, then $\operatorname{cok}(M(n))$ is trivial if and only if $M(n)$ is a non-singular matrix when reduced mod p. More generally, the corank of the reduction of $M(n)$ modulo p is the rank of the cokernel of $M(n)$. There is a long history of work on singularity and ranks of the random matrices we consider above mod p, including results of Kozlov [Koz66], Kovalenko and Levitskaja [KL75], Charlap, Rees, and Robbins [CRR90] (first proving Theorem 1.2 in the case that B is the trivial group), Kahn and Komlós [KK01], and Maples [Map10]. However, even our result on ranks (Corollary 3.5), that for $M(n)$ as in Theorem 1.2,

$$\lim_{n\to\infty} \mathbb{P}\big(\operatorname{rank}\big(M(n)\big) = n-k\big) = p^{-k^2}\prod_{i=1}^{k}\big(1-p^{-i}\big)^{-2}\prod_{i\geq 1}\big(1-p^{-i}\big)$$

appears to be new with our hypotheses. The realization that the cokernel distribution, and not just the ranks, should also be insensitive to the distributions of the entries of the matrices is due to Tao and Maples (see [Map13] for some interesting work towards Theorem 1.2).

This universality of certain statistics of random matrices under changes to the entry distribution of the matrices is an important theme in the study of random matrices. For example, the best upper bounds on the singularity probability of discrete random matrices with independent entries in characteristic 0, due to Bourgain, Vu, and Wood [BVW10], are insensitive to the actual values the entries take (as long as they are not too concentrated).

To prove our main result, we first determine the moments of the cokernel distributions, and from that determine the distributions themselves. Our specific approach was developed in [Woo14] for the case of symmetric matrices. In this paper, we are able to use a much simplified version of that in [Woo14] since the entries of our matrices are independent. To find the moments $\mathbb{E}(\#\operatorname{Sur}(\operatorname{cok}(M(n)), G))$, we prove inverse Littlewood-Offord theorems (Lemmas 2.1 and 2.7). These both say that if values of several linear functions of our n independent variables are not close to equidistributed, then the linear functions are close to having extra structure. The extra structure is analogous to having a linear dependence in rows of a matrix after deleting a small number of columns, but since our linear algebra is not always over a field there are many layers to the type of dependence we can have, which are captured by our notion of *δ-depth*. Inverse Littlewood-Offord Theorems are a key component in the most recent work on singularity probability of discrete random matrices in characteristic 0, both [BVW10] mentioned above and the earlier work of Tao and Vu [TV07]. (See the papers of Tao and Vu [TV10] and Nguyen and Vu [NV11] for the most recent inverse Littlewood-Offord Theorems in characteristic 0, as well as a guide to the extensive previous work on the problem.) However, there

are significant differences in the actual mathematics of these theorems in characteristic 0 versus characteristic p, since in characteristic 0 one doesn't expect any kind of equidistribution, but rather just a good upper bound on the probabilities. Maples [Map13] proves a Littlewood-Offord Theorem in characteristic p that is not strong enough for our purposes for fixed p, but does have the advantage of uniformity in p.

To finally determine our cokernel distribution from the moments, we can't rely on the usual probabilistic methods such as Carleman's condition (since our moments are too big—our kth moment is of order $p^{k^2/2}$). However, we use a specifically tailored result from [Woo14] that in our cases shows that the moments we obtain determine a unique distribution. This situation of needing to show that fast growing moments of random abelian groups determine the distribution of the groups has arisen before in number theory, both in Cohen-Lenstra problems, e.g., in the work of Fouvry and Klüners [FK06] and Ellenberg, Venkatesh, and Westerland [EVW09], and in a related problem about Selmer groups in work of Heath-Brown [HB94]. Ellenberg, Venkatesh, and Westerland [EVW09] make progress towards proving the function field analogue of the Cohen-Lenstra heuristics by proving new homological stability theorems that determine some of the moments of the relevant class groups.

1.1. Further notation. We use $[n]$ to denote $\{1,\dots,n\}$. We write $\mathrm{Hom}(A,B)$ and $\mathrm{Sur}(A,B)$ for the set of homomorphisms and surjective homomorphisms, respectively, from A to B. We write $\mathbb{P}$ for probability and $\mathbb{E}$ for expected value. We write $\exp(x)$ for the exponential function e^x.

Acknowledgments. The author thanks Nathan Kaplan, John Voight, and the referee for useful comments on an earlier draft of this paper.

2. Finding the moments. We will study integral matrices by reducing them mod a for all integers $a \geq 2$ (and analogously matrices over $\mathbb{Z}_p$ by reducing them mod p^k for all positive integers k). Throughout this section, we work with an integer $a \geq 2$, and let $R = \mathbb{Z}/a\mathbb{Z}$. Further, throughout this section, we work with a fixed non-negative integer u. For each positive integer n, we will study random $n \times (n+u)$ matrices M with entries valued in R. These are the reductions mod a of the matrices $M(n)$ in the introduction, but we will drop the n in the notation when it is possible to do so without causing confusion. We let $M_1,\dots,M_{n+u}$ be the columns of M (which are random vectors valued in R^n), and M_{ij} the entries of M (so that the entries of M_j are M_{ij}).

The following definition captures the two hypotheses of Theorem 1.2: independence of entries and entries not too concentrated.

Definition 1. Let $\epsilon > 0$ be a real number. Let T be either $\mathbb{Z}$, or a completion or quotient of $\mathbb{Z}$. A random variable y valued in T is *ϵ-balanced* if for every maximal

ideal $\wp$ of T and for every $r \in T/\wp$ we have $\mathbb{P}(y \equiv r \pmod{\wp}) \leq 1-\epsilon$ (e.g., $y \in R$ is *ϵ-balanced* if for every prime $p \mid a$ and $r \in \mathbb{Z}/p\mathbb{Z}$ we have $\mathbb{P}(y \equiv r \pmod{p}) \leq 1-\epsilon$). A random vector or matrix with entries in T is *ϵ-balanced* if its entries are independent and ϵ-balanced.

Throughout this section we will use the following notation. We let $V = R^n$ with standard basis v_i and $W = R^{n+u}$ with standard basis w_j. Note that for each $\sigma \subset [n]$, V has a distinguished submodule $V_{\backslash\sigma}$ generated by the v_i with $i \notin \sigma$. (So $V_{\backslash\sigma}$ comes from not using the σ coordinates.) We view M as an element of $\mathrm{Hom}(W,V)$, and its columns M_j as elements of V so that $M_j = Mw_j = \sum_i M_{ij}v_i$. Let G be a finite abelian group with exponent dividing a. We have $\operatorname{cok} M = V/MW$.

To investigate the moments $\mathbb{E}(\#\mathrm{Sur}(\operatorname{cok} M, G))$, we recognize that each such surjection lifts to a surjection $V \to G$ and so we have

$$\mathbb{E}(\#\mathrm{Sur}(\operatorname{cok} M, G)) = \sum_{F \in \mathrm{Sur}(V,G)} \mathbb{P}(F(MW) = 0). \tag{3}$$

If M is ϵ-balanced, then by the independence of columns, we have

$$\mathbb{P}(F(MW) = 0) = \prod_{j=1}^{n+u} \mathbb{P}(F(M_j) = 0).$$

So we aim to estimate these probabilities $\mathbb{P}(F(M_j) = 0)$. We will first estimate these for the vast majority of F, which satisfy the following helpful property.

Definition 2. Given integers $a \geq 2$ and $n \geq 1$, let $V = (\mathbb{Z}/a\mathbb{Z})^n$. Let G be a finite abelian group with exponent dividing a. We say that $F \in \mathrm{Hom}(V,G)$ is a *code* of distance w if for every $\sigma \subset [n]$ with $|\sigma| < w$, we have $FV_{\backslash\sigma} = G$. In other words, F is not only surjective, but would still be surjective if we throw out (any) fewer than w of the standard basis vectors from V. (If a is prime, so that R is a field, then this is equivalent to the transpose map $F : \mathrm{Hom}(G,R) \to \mathrm{Hom}(V,R)$ being injective and its image $\mathrm{im}(F) \subset \mathrm{Hom}(V,R)$ being a linear code of distance w in the usual sense.)

LEMMA 2.1. *Let a be an integer with $a \geq 2$. Let G be a finite abelian group with exponent dividing a. Let $\epsilon > 0$ and $\delta > 0$ be real numbers. Let n be a positive integer. Let X be an ϵ-balanced random vector valued in $V = (\mathbb{Z}/a\mathbb{Z})^n$. Let $F \in \mathrm{Hom}(V,G)$ be a code of distance δn and let A be an element of G. We have*

$$\left|\mathbb{P}(FX = A) - |G|^{-1}\right| \leq \exp\left(-\epsilon\delta n/a^2\right).$$

To prove Lemma 2.1, we will use the discrete Fourier transform and the following basic estimate.

LEMMA 2.2. *Let $\epsilon > 0$ be a real number, and $a \geq 2$ an integer. Let ζ be a primitive ath root of unity. Let y be an ϵ-balanced random variable valued in $\mathbb{Z}/a\mathbb{Z}$, and let m be an integer such that $\zeta^m \neq 1$. Then $|\mathbb{E}(\zeta^{my})| \leq \exp(-\epsilon/a^2)$.*

Proof. This is proven in [Woo14, Proof of Lemma 4.1]. Briefly, the greatest $|\mathbb{E}(\zeta^y)|$ could be was if ζ^y was one ath root of unity $1-\epsilon$ of the time, and a consecutive (around the unit circle) ath root of unity the rest of the time. □

Proof of Lemma 2.1. Let ζ be a primitive ath root of unity. Let X_i be the entries of X. We have, by the discrete Fourier transform,

$$\begin{aligned}\mathbb{P}(FX = A) &= |G|^{-1} \sum_{C \in \mathrm{Hom}(G,R)} \mathbb{E}\big(\zeta^{C(FX-A)}\big) \\ &= |G|^{-1} + |G|^{-1} \sum_{C \in \mathrm{Hom}(G,R)\setminus\{0\}} \mathbb{E}\big(\zeta^{C(-A)}\big) \prod_{1 \leq i \leq n} \mathbb{E}\big(\zeta^{C(F(v_i))X_i}\big).\end{aligned}$$

Since F is a code, for $C \in \mathrm{Hom}(G,R) \setminus \{0\}$ there must be at least δn values of i such that $F(v_i) \notin \ker C$. For these i, we have $C(F(v_i)) \neq 0$. So using Lemma 2.2, we have for each $C \in \mathrm{Hom}(G,R) \setminus \{0\}$,

$$\left| \mathbb{E}\big(\zeta^{C(-A)}\big) \prod_{1 \leq i \leq n} \mathbb{E}\big(\zeta^{C(F(v_i))X_i}\big) \right| \leq \exp\big(-\epsilon\delta n/a^2\big).$$

The lemma follows. □

We then put these estimates for columns together using a simple inequality.

LEMMA 2.3. *If we have an integer $m \geq 2$ and real numbers $x \geq 0$ and y such that $|y|/x \leq 2^{1/(m-1)} - 1$ and $x + y \geq 0$, then*

$$|(x+y)^m - x^m| \leq 2mx^{m-1}|y|.$$

Proof. We wish to show

$$x^m - 2mx^{m-1}|y| \leq (x+y)^m \leq x^m + 2mx^{m-1}|y|.$$

We can assume $x = 1$ by homogeneity. If $y \geq 0$, then the left inequality is trivial. Then note the middle and right expressions are equal when $y = 0$ and the derivative in y of the middle is at most the derivative of the right when $0 \leq y \leq 2^{1/(m-1)} - 1$. Thus for $0 \leq y \leq 2^{1/(m-1)} - 1$, the lemma follows. If $y \leq 0$, then the right inequality is trivial. For all $-1 \leq y \leq 0$, the derivative in y of the left expression is at least the derivative of the middle expression, and the two expressions are equal when $y = 0$. Thus for $-1 \leq y \leq 0$, the lemma follows. □

LEMMA 2.4. *Let a be an integer with $a \geq 2$. Let G be a finite abelian group with exponent dividing a. Let u be a non-negative integer. Let $\epsilon > 0$ and $\delta > 0$*

be real numbers. Then there are real numbers $c, K > 0$, depending on a, G, u, ϵ, and δ, such that, for every positive integer n, every ϵ-balanced random matrix M valued in $\mathrm{Hom}(W,V)$, every code $F \in \mathrm{Hom}(V,G)$ of distance δn, and every $A \in \mathrm{Hom}(W,G)$, we have

$$\left|\mathbb{P}(FM = A) - |G|^{-n-u}\right| \leq \frac{K \exp(-cn)}{|G|^{n+u}},$$

where $V = (\mathbb{Z}/a\mathbb{Z})^n$ and $W = (\mathbb{Z}/a\mathbb{Z})^{n+u}$.

Proof. We are given a, G, u, ϵ and δ, and throughout the proof we will take n sufficiently large given these values. Let w_i be the standard basis of W. Note that $\mathbb{P}(FM = A) = \prod_{i=1}^{n+u} \mathbb{P}(FM_i = A(w_i))$ since M has independent columns. In particular

$$\min_i \mathbb{P}(FM_i = A(w_i))^{n+u} \leq \mathbb{P}(FM = A) \leq \max_i \mathbb{P}(FM_i = A(w_i))^{n+u}. \tag{4}$$

For $1 \leq i \leq n+u$, from Lemma 2.1 we have

$$\left|\mathbb{P}(FM_i = A(w_i)) - |G|^{-1}\right| \leq \exp(-\epsilon\delta n/a^2).$$

For n sufficiently large we have

$$\exp(-\epsilon\delta n/a^2)|G| \leq \log 2/(n+u-1).$$

For $n+u-1 > 0$, we have $\log 2/(n+u-1) \leq e^{\log 2/(n+u-1)} - 1$. Thus, for n sufficiently large we have

$$\exp(-\epsilon\delta n/a^2)|G| \leq 2^{1/(n+u-1)} - 1.$$

Thus, for n sufficiently large we can apply Lemma 2.3 with $m = n+u$, $x = |G|^{-1}$ and $y = \mathbb{P}(FM_i = A(w_i)) - |G|^{-1}$ to obtain

$$\begin{aligned}&\left|\mathbb{P}\big(FM_i = A\big(w_i\big)\big)^{n+u} - |G|^{-n-u}\right| \\ &\quad \leq 2(n+u)|G|^{-n-u+1}\left|\mathbb{P}\big(FM_i = A\big(w_i\big)\big) - |G|^{-1}\right|.\end{aligned}$$

Thus

$$\left|\mathbb{P}\big(FM_i = A\big(w_i\big)\big)^{n+u} - |G|^{-n-u}\right| \leq 2(n+u)|G|^{-n-u+1}\exp\big(-\epsilon\delta n/a^2\big).$$

From Equation (4) and the fact that $|z - |G|^{-n-u}|$ is a convex function in z, it follows that

$$\left|\mathbb{P}(FM = A) - |G|^{-n-u}\right| \leq 2(n+u)|G|^{-n-u+1}\exp(-\epsilon\delta n/a^2).$$

So for any c such that $0 < c < \epsilon\delta/a^2$, for n sufficiently large (now also given c) we have

$$(n+u)\exp\big(-\epsilon\delta n/a^2\big) \le \exp(-cn),$$

and thus

$$\big|\mathbb{P}(FM = A) - |G|^{-n-u}\big| \le 2|G|\frac{\exp(-cn)}{|G|^{n+u}}. \tag{5}$$

We let K be the maximum of $2|G|$ and $|\mathbb{P}(FM = A) - |G|^{-n-u}|/(\exp(-cn)/|G|^{n+u})$ for all the finitely many values of n such that Equation (5) does not hold. The lemma follows. □

So far, we have dealt with $F \in \mathrm{Hom}(V,G)$ that are codes. Unfortunately, it is not sufficient to partition $\mathrm{Hom}(V,G)$ into codes and non-codes. We need a more delicate partition of $\mathrm{Hom}(V,G)$, indexed by the subgroups of G. This division can be approximately understood as separating the F based on what largest size subgroup they are a code for. For a positive integer D with prime factorization $\prod_i p_i^{e_i}$, let $\ell(D) = \sum_i e_i$. The following concept was introduced in [Woo14]. Since $V_{\setminus\sigma}$ is a subgroup of V, for $F \in \mathrm{Hom}(V,G)$, the image $F(V_{\setminus\sigma})$ is a subgroup of G.

Definition 3. For a real $\delta > 0$, the *δ-depth* of an $F \in \mathrm{Hom}(V,G)$ is the maximal positive integer D such that there is a $\sigma \subset [n]$ with $|\sigma| < \ell(D)\delta n$ such that $D = [G : F(V_{\setminus\sigma})]$, or is 1 if there is no such D.

Remark 2.5. In particular, if the δ-depth of F is 1, then for every $\sigma \subset [n]$ with $|\sigma| < \delta n$, we have that $F(V_{\setminus\sigma}) = G$ (as otherwise $\ell([G : F(V_{\setminus\sigma})]) \ge 1$), and so we see that F is a code of distance δn. Further, if the δ-depth of F is greater than 1, since $\ell(D) \ge 1$, we see that F is not a code of distance δn.

We have a bound for the number of $F \in \mathrm{Hom}(V,G)$ that are of δ-depth D.

LEMMA 2.6. (Count F of given δ-depth, Lemma 5.2 of [Woo14]) *Let a be an integer with $a \ge 2$. Let G be a finite abelian group with exponent dividing a. There is a constant K, depending on a and G, such that for all positive integers n, all integers $D > 1$, and all real numbers $\delta > 0$, the number of $F \in \mathrm{Hom}(V,G)$ of δ-depth D is at most*

$$K\binom{n}{\lceil \ell(D)\delta n\rceil - 1}|G|^n|D|^{-n+\ell(D)\delta n},$$

where $V = (\mathbb{Z}/a\mathbb{Z})^n$.

Now for each δ-depth, we will get a bound on $\mathbb{P}(FM = 0)$ for F of that δ-depth. For smaller δ-depths, we will have better bounds.

LEMMA 2.7. (Bound probability for column given δ-depth) *Let a be an integer with $a \geq 2$. Let G be a finite abelian group with exponent dividing a. Let $\epsilon > 0$ and $\delta > 0$ be real numbers. Let n be a positive integer and $V = (\mathbb{Z}/a\mathbb{Z})^n$. If $F \in \mathrm{Hom}(V,G)$ has δ-depth $D > 1$ and $[G : F(V)] < D$, then for all ϵ-balanced random vectors X valued in V,*

$$\mathbb{P}(FX = 0) \leq (1-\epsilon)\left(D|G|^{-1} + \exp\left(-\epsilon\delta n/a^2\right)\right).$$

Proof. Let V have standard basis v_i. Pick a $\sigma \subset [n]$ with $|\sigma| < \ell(D)\delta n$ such that $D = [G : F(V_{\setminus\sigma})]$. Let $F(V_{\setminus\sigma}) = H$. Since $[G : F(V)] < D$, the set σ is non-empty. We have $FX = \sum_{i\notin\sigma} F(v_i)X_i + \sum_{i\in\sigma} F(v_i)X_i$. So

$$\mathbb{P}(FX = 0) = \mathbb{P}\left(\sum_{i\in\sigma} F(v_i)X_i \in H\right) \times \mathbb{P}\left(\sum_{i\notin\sigma} F(v_i)X_i = -\sum_{i\in\sigma} F(v_i)X_i \Big| \sum_{i\in\sigma} F(v_i)X_i \in H\right).$$

For the first factor, we note that since $[G : F(V)] < D$, there must be some $i \in \sigma$ with the reduction $F(v_i) \neq 0 \in G/H$. Thus conditioning on all other X_k for $k \neq i$, by the ϵ-balanced assumption on X, we have that $\mathbb{P}(\sum_{i\in\sigma} F(v_i)X_i \in H) \leq 1-\epsilon$.

Then, we note that the restriction of F to $V_{\setminus\sigma}$ is a code of distance δn in $\mathrm{Hom}(V_{\setminus\sigma}, H)$. (If it were not, then by eliminating σ and $< \delta n$ indices, we would eliminate $< (\ell(D)+1)\delta n$ indices and have an image whose index is strictly divisible by D, contradicting the δ-depth of F.) So conditioning on the X_i with $i \in \sigma$, we can estimate the conditional probability above using Lemma 2.1 on $F \in \mathrm{Hom}(V_{\setminus\sigma}, H)$:

$$\mathbb{P}\left(\sum_{i\notin\sigma} F(v_i)X_i = -\sum_{i\in\sigma} F(v_i)X_i \Big| \sum_{i\in\sigma} F(v_i)X_i \in H\right) \leq |H|^{-1} + \exp\left(-\epsilon\delta n/a^2\right).$$

The lemma follows. □

LEMMA 2.8. (Bound probability for matrix given δ-depth) *Let a be an integer with $a \geq 2$. Let G be a finite abelian group with exponent dividing a. Let u be a non-negative integer. Let $\epsilon > 0$ and $\delta > 0$ be real numbers. Then there is a real number K, depending on a, G, u, ϵ, and δ, such that for every positive integer n, every $F \in \mathrm{Hom}(V,G)$ of δ-depth $D > 1$ with $[G : F(V)] < D$ (e.g., the latter is true if $F(V) = G$), and every ϵ-balanced random matrix M valued in $\mathrm{Hom}(W,V)$, we have*

$$\mathbb{P}(FM = 0) \leq K\exp(-\epsilon n)D^n|G|^{-n},$$

where $V = (\mathbb{Z}/a\mathbb{Z})^n$ and $W = (\mathbb{Z}/a\mathbb{Z})^{n+u}$.

Proof. By the independence of the columns of M, we have

$$\mathbb{P}(FM=0)=\prod_{i=1}^{n+u}\mathbb{P}(FM_i=0).$$

By Lemma 2.7 for all i with $1\le i\le n+u$,

$$\mathbb{P}(FM_i=0)\le(1-\epsilon)\left(D|G|^{-1}+\exp\left(-\epsilon\delta n/a^2\right)\right).$$

Thus

$$\mathbb{P}(FM=0)\le(1-\epsilon)^{n+u}\left(D|G|^{-1}+\exp\left(-\epsilon\delta n/a^2\right)\right)^{n+u}.$$

We apply Lemma 2.3 with $x=D|G|^{-1}$ and $y=\exp(-\epsilon\delta n/a^2)$, and as long as n is sufficiently large given a,G,u,ϵ and δ we have $|y|/x\le 2^{1/(n+u-1)}-1$ as in the proof of Lemma 2.4. Thus for n sufficiently large, Lemma 2.3 gives

$$\begin{aligned}&\left(D|G|^{-1}+\exp\left(-\epsilon\delta n/a^2\right)\right)^{n+u}-D^{n+u}|G|^{-n-u}\\&\quad\le 2(n+u)\exp\left(-\epsilon\delta n/a^2\right)D^{n+u-1}|G|^{-n-u+1}.\end{aligned}$$

Thus, for n sufficiently large, we have

$$\begin{aligned}&\mathbb{P}(FM=0)\\&\le(1-\epsilon)^{n+u}\left(D^{n+u}|G|^{-n-u}+2(n+u)\exp(-\epsilon\delta n/a^2)D^{n+u-1}|G|^{-n-u+1}\right)\\&\le\exp(-\epsilon(n+u))\left(D^{n+u}|G|^{-n-u}+2D^{n+u-1}|G|^{-n-u+1}\right).\end{aligned}$$

We take K to be the maximum of $\exp(-\epsilon(u)D^u|G|^{-u})(1+2|G|/D)$ and $\mathbb{P}(FM=0)/(\exp(-\epsilon n)D^n|G|^{-n})$ over all the finitely many n such that the above does not hold. The lemma follows. □

Now we can combine the estimates we have for $\mathbb{P}(FM=0)$ for F of various δ-depth with the bounds we have on the number of F of each δ-depth to obtain our main result on the moments of cokernels of random matrices.

THEOREM 2.9. *Let a be an integer with $a\ge 2$. Let G be a finite abelian group with exponent dividing a. Let u be a non-negative integer. Let $\epsilon>0$ be a real number. Then there are $c,K>0$, depending on a,G,u, and ϵ, such that the following holds. Let n be a positive integer and let M be an ϵ-balanced $n\times(n+u)$ random matrix with entries valued in $\mathbb{Z}/a\mathbb{Z}$. We have*

$$\left|\mathbb{E}(\#\mathrm{Sur}(\mathrm{cok}(M),G))-|G|^{-u}\right|\le Ke^{-cn}.$$

Proof. By Equation (3), it suffices to estimate $\sum_{F\in\mathrm{Sur}(V,G)}\mathbb{P}(FM=0)$. First, we will pick some parameters that will be needed in the proof. We choose a positive real $d<\min(\epsilon,\log(2))$. Given G and d, we will pick a real number $\delta>0$

sufficiently small, such that there is a real number $K > 0$, such that for all positive integers n

$$\binom{n}{\lceil \ell(|G|)\delta n\rceil - 1}|G|^{\ell(|G|)\delta n}\exp(-\epsilon n) \leq Ke^{-dn}$$

and

$$\binom{n}{\lceil \ell(|G|)\delta n\rceil - 1}2^{-n+\ell(|G|)\delta n} \leq Ke^{-dn}.$$

(This is possible because $\binom{n}{\alpha n} \leq 2^{H(\alpha)n}$, where $H(\alpha)$ is the binary entropy of α and goes to 0 as $\alpha \to 0$.) Below, we will let the value of K change in each line, as long as it is a positive real number depending only on $a, G, u, \epsilon, \delta$ and d. Using Lemmas 2.6 and 2.8 we have, for every positive integer n,

$$\begin{aligned}
&\sum_{\substack{F\in \mathrm{Sur}(V,G)\\ F \text{ not code of distance } \delta n}} \mathbb{P}(FX = 0)\\
&\quad= \sum_{\substack{D>1\\ D|\#G}} \sum_{\substack{F\in \mathrm{Sur}(V,G)\\ F\ \delta\text{-depth } D}} \mathbb{P}(FX = 0)\\
&\quad\leq \sum_{\substack{D>1\\ D|\#G}} K\binom{n}{\lceil \ell(D)\delta n\rceil - 1}|G|^n D^{-n+\ell(D)\delta n}\exp(-\epsilon n)D^n|G|^{-n}\\
&\quad\leq \sum_{\substack{D>1\\ D|\#G}} K\binom{n}{\lceil \ell(D)\delta n\rceil - 1}D^{\ell(D)\delta n}\exp(-\epsilon n)\\
&\quad\leq K\binom{n}{\lceil \ell(|G|)\delta n\rceil - 1}|G|^{\ell(|G|)\delta n}\exp(-\epsilon n)\\
&\quad\leq Ke^{-dn},
\end{aligned}$$

by our choice of δ.

Also, from Lemma 2.6, we have, for every positive integer n,

$$\begin{aligned}
\sum_{\substack{F\in \mathrm{Sur}(V,G)\\ F \text{ not code of distance } \delta n}} |G|^{-n-u} &= \sum_{\substack{D>1\\ D|\#G}} \sum_{\substack{F\in \mathrm{Sur}(V,G)\\ F\ \delta\text{-depth } D}} |G|^{-n-u}\\
&\leq \sum_{\substack{D>1\\ D|\#G}} K\binom{n}{\lceil \ell(D)\delta n\rceil - 1}|G|^n|D|^{-n+\ell(D)\delta n}|G|^{-n}\\
&\leq K\binom{n}{\lceil \ell(|G|)\delta n\rceil - 1}2^{-n+\ell(|G|)\delta n}\\
&\leq Ke^{-dn}.
\end{aligned}$$

We also have, for every positive integer n,

$$\begin{aligned}\sum_{F\in\mathrm{Hom}(V,G)\setminus\mathrm{Sur}(V,G)} |G|^{-n-u} &= \sum_{H \text{ proper s.g of } G} \sum_{F\in\mathrm{Hom}(V,H)} |G|^{-n-u}\\ &\le \sum_{H \text{ proper s.g of } G} |H|^{n+u}|G|^{-n-u}\\ &\le Ke^{-dn}.\end{aligned}$$

Using Lemma 2.4 we have a real number $c>0$ and can further choose a real $K>0$, both depending only on $a, G, u, \epsilon, \delta$, and d, such that for every positive integer n, we have

$$\sum_{\substack{F\in\mathrm{Sur}(V,G)\\ F \text{ code of distance } \delta n}} \left|\mathbb{P}(FX=0) - |G|^{-n+u}\right| \le Ke^{-cn}.$$

If necessary, we take c smaller so $c\le d$. In conclusion, for every positive integer n,

$$\begin{aligned}&\left|\left(\sum_{F\in\mathrm{Sur}(V,G)} \mathbb{P}(FX=0)\right) - |G|^{-u}\right|\\ &= \left|\left(\sum_{F\in\mathrm{Sur}(V,G)} \mathbb{P}(FX=0)\right) - \left(\sum_{F\in\mathrm{Hom}(V,G)} |G|^{-n-u}\right)\right|\\ &\le \sum_{\substack{F\in\mathrm{Sur}(V,G)\\ F \text{ code of distance } \delta n}} \left|\mathbb{P}(FX=0) - |G|^{-n-u}\right| + \sum_{\substack{F\in\mathrm{Sur}(V,G)\\ F \text{ not code of distance } \delta n}} \mathbb{P}(FX=0)\\ &\quad + \sum_{\substack{F\in\mathrm{Hom}(V,G)\\ F \text{ not code of dist. } \delta n}} |G|^{-n-u}\\ &\le Ke^{-cn}.\end{aligned}$$

□

3. Moments determine the distribution. We use the following theorem to determine the asymptotic distribution of $\mathrm{cok}(M)$ as $n\to\infty$ from the moments in Theorem 2.9.

THEOREM 3.1. (cf. Theorem 8.3 in [Woo14]) *Let $\{X_n\}_{n\ge1}$ and $\{Y_n\}_{n\ge1}$ be sequences of random finitely generated abelian groups X_n and Y_n as n ranges over positive integers. Let a be a positive integer and $\mathcal{A}$ be the set of (isomorphism classes of) abelian groups with exponent dividing a. Suppose that for every $G\in\mathcal{A}$, we have a real number $M_G\le|\wedge^2 G|$ such that*

$$\lim_{n\to\infty} \mathbb{E}(\#\mathrm{Sur}(X_n,G)) = M_G.$$

Then for every $H \in \mathcal{A}$, the limit $\lim_{n\to\infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)$ exists, and for all $G \in \mathcal{A}$ we have

$$\sum_{H\in A} \lim_{n\to\infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H)\#\mathrm{Sur}(H,G) = M_G.$$

If for every $G \in \mathcal{A}$, we also have $\lim_{n\to\infty} \mathbb{E}(\#\mathrm{Sur}(Y_n,G)) = M_G$, then, we have that for every every $H \in \mathcal{A}$

$$\lim_{n\to\infty} \mathbb{P}(X_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H) = \lim_{n\to\infty} \mathbb{P}(Y_n \otimes \mathbb{Z}/a\mathbb{Z} \simeq H).$$

Let $a \geq 2$ be an integer and u be a non-negative integer. We construct a random abelian group according to Cohen and Lenstra's distribution for each u as follows. Let P_a be the set of primes dividing a. Independently for each p, we have a random finite abelian p-group $Y_p(u)$ given by taking each finite abelian p-group B with probability $\frac{\prod_{j=1}^{\infty}(1-p^{-j-u})}{|B|^u|\mathrm{Aut}(B)|}$. We then form a random group $Y_a(u)$ by taking $Y_a(u) = \prod_{p\in P_a} Y_p(u)$.

LEMMA 3.2. *Let $a \geq 2$ be a positive integer. Let u be a non-negative integer and $Y_a(u)$ the random group defined just above. For every finite abelian group G with exponent dividing a, we have*

$$\mathbb{E}(\#\mathrm{Sur}(Y_a(u),G)) = |G|^{-u}.$$

In particular, the proof of Lemma 3.2 in the case that G is the trivial group shows that the probabilities given to define $Y_p(u)$ sum to 1.

Proof. By factoring over primes $p \in P$, we can reduce to the case when $P = \{p\}$. Let $\mathcal{A}$ be the set of finite abelian p-groups. A proposition of Cohen and Lenstra [CL84, Proposition 4.1 (ii)] (in the case $k = \infty$ and $K = G$) says that for every positive integer i,

$$\sum_{B\in\mathcal{A},\,|B|=p^i} \frac{|\mathrm{Sur}(B,G)|}{|\mathrm{Aut}(G)||\mathrm{Aut}(B)|} = \sum_{B\in\mathcal{A},\,|B|=p^i/|G|} \frac{1}{|\mathrm{Aut}(G)||\mathrm{Aut}(B)|}.$$

We can multiply the above by $|\mathrm{Aut}(G)|p^{-iu}$ and sum over all i to obtain

$$\sum_{B\in\mathcal{A}} \frac{|\mathrm{Sur}(B,G)|}{|B|^u|\mathrm{Aut}(B)|} = |G|^{-u} \sum_{B\in\mathcal{A}} \frac{1}{|B|^u|\mathrm{Aut}(B)|}.$$

By another result of Cohen and Lenstra [CL84, Corollary 3.7 (i)] (in the case $s = u$ and $k = \infty$), we have $\sum_{B\in\mathcal{A}} |B|^{-u}|\mathrm{Aut}(B)|^{-1} = \prod_{j\geq 1}(1-p^{-j-u})^{-1}$, and the lemma follows. □

We now find the distribution of our cokernels by comparing their moments to those of Y.

COROLLARY 3.3. (of Theorem 2.9 and Theorem 3.1) *Let $a \geq 2$ be a positive integer. Let G be a finite abelian group with exponent dividing a. Let u be a non-negative integer. Let $\epsilon > 0$ be a real number. For every positive integer n, let $M(n)$ be an ϵ-balanced random matrix valued in $M_{n\times(n+u)}(\mathbb{Z})$. For the random group $Y_a(u)$ defined just above Lemma 3.2, we have*

$$\lim_{n\to\infty} \mathbb{P}(\mathrm{cok}(M(n)) \otimes \mathbb{Z}/a\mathbb{Z} \simeq G) = \mathbb{P}(Y_a(u) \otimes \mathbb{Z}/a\mathbb{Z} \simeq G).$$

We have the same result if a is a power of p and $M(n)$ is a random matrix valued in $M_{n\times(n+u)}(\mathbb{Z}_p)$.

In particular, we can conclude the following, which proves Theorems 1.2 and 1.3.

COROLLARY 3.4. *Let u be a non-negative integer and $\epsilon > 0$ be a real number. For every positive integer n, let $M(n)$ be an ϵ-balanced random matrix valued in $M_{n\times(n+u)}(\mathbb{Z})$ (resp, $M(n) \in M_{n\times(n+u)}(\mathbb{Z}_p)$ for a prime p). Let B be a finite abelian group (resp., finite abelian p-group). Let P be a finite set of primes including all those dividing $|B|$ (resp., $P = \{p\}$). Let $H_P := \prod_{p\in P} H_p$ be the product of the Sylow p-subgroups of H for $p \in P$. Then*

$$\lim_{n\to\infty} \mathbb{P}(\mathrm{cok}(M(n))_P \simeq B) = \frac{1}{|B|^u |\mathrm{Aut}(B)|} \prod_{p\in P} \prod_{k=1}^{\infty} (1 - p^{-k-u}).$$

Proof. Note that if B is a finite abelian group with exponent that has prime factorization $\prod_{p\in P} p^{e_p}$, then if we take $a = \prod_{p\in P} p^{e_p+1}$, for any finitely generated abelian group H, we have $H \otimes \mathbb{Z}/a\mathbb{Z} \simeq G$ if and only if $H_P \simeq G$.

So the corollary follows from Corollary 3.3 and the construction of $Y_a(u)$. □

As in [Woo14, Corollary 9.3], it follows that when $u = 0$, then for M as in Corollary 3.4 and any finite abelian group G we have $\lim_{n\to\infty} \mathbb{P}(\mathrm{cok}(M) \simeq B) = 0$. This agrees with the (known) prediction of the Cohen-Lenstra distribution for imaginary quadratic fields that any particular group appears as a class group with density 0. Also taking $a = p$ for a prime p in Corollary 3.3, we conclude the following on the distribution of p-ranks.

COROLLARY 3.5. *Let u be a non-negative integer, p be a prime and $\epsilon > 0$ be a real number. For every positive integer n, let $M(n) \in M_{n\times(n+u)}(\mathbb{Z}/p\mathbb{Z})$ be an ϵ-balanced random matrix. For every non-negative integer k, we have*

$$\lim_{n\to\infty} \mathbb{P}(\mathrm{rank}(M(n)) = n-k) = p^{-k(k+u)} \prod_{i=1}^{k} (1-p^{-i})^{-1} \prod_{i=1}^{k+u} (1-p^{-i})^{-1} \prod_{i\geq 1} (1-p^{-i}).$$

Proof. We apply Theorem 2.9 with $a = p$ and Theorem 3.1 with $a = p$ to $\mathrm{cok}(M)$ and $Y(u,p)$. We can read off the rank distribution of Y from

[CL84][Theorem 6.3]. (Alternatively, instead of $Y(u,p)$ we could use cokernels of $H_n \in M_{n\times(n+u)}(\mathbb{Z}/p\mathbb{Z})$ from the uniform distribution and use the elementary count of matrices over $\mathbb{Z}/p\mathbb{Z}$ of a given rank.) □

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN-MADISON, 480 LINCOLN DRIVE, MADISON, WI 53705
E-mail: mmwood@math.wisc.edu

REFERENCES

[BVW10] J. Bourgain, V. H. Vu, and P. M. Wood, On the singularity probability of discrete random matrices, *J. Funct. Anal.* **258** (2010), no. 2, 559–603.

[CRR90] L. S. Charlap, H. D. Rees, and D. P. Robbins, The asymptotic probability that a random biased matrix is invertible, *Discrete Math.* **82** (1990), no. 2, 153–163.

[CL84] H. Cohen and H. W. Lenstra Jr., Heuristics on class groups of number fields, *Number Theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, *Lecture Notes in Math.*, vol. 1068, Springer-Verlag, Berlin, 1984, pp. 33–62.

[EVW09] J. S. Ellenberg, A. Venkatesh, and C. Westerland, Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields, *Ann. of Math. (2)* **183** (2016), no. 3, 729–786.

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

[FW89] E. Friedman and L. C. Washington, On the distribution of divisor class groups of curves over a finite field, *Théorie des nombres (Quebec, PQ, 1987)*, de Gruyter, Berlin, 1989, pp. 227–239.

[HB94] D. R. Heath-Brown, The size of Selmer groups for the congruent number problem. II. With an appendix by P. Monsky, *Invent. Math.* **118** (1994), no. 2, 331–370.

[KK01] J. Kahn and J. Komlós, Singularity probabilities for random matrices over finite fields, *Combin. Probab. Comput.* **10** (2001), no. 2, 137–157.

[KL75] I. N. Kovalenko and A. A. Levitskaja, Limiting behavior of the number of solutions of a system of random linear equations over a finite field and a finite ring, *Dokl. Akad. Nauk SSSR* **221** (1975), no. 4, 778–781.

[Koz66] M. V. Kozlov, On the rank of matrices with random Boolean elements, *Soviet Math. Dokl.* **7** (1966), 1048–1051.

[Map10] K. Maples, Singularity of random matrices over finite fields, preprint, https://arxiv.org/abs/1012.2372, 2010.

[Map13] ———, Cokernels of random matrices satisfy the Cohen-Lenstra heuristics, preprint, https://arxiv.org/abs/1301.1239, 2013.

[NV11] H. Nguyen and V. Vu, Optimal inverse Littlewood-Offord theorems, *Adv. Math.* **226** (2011), no. 6, 5298–5319.

[TV07] T. Tao and V. Vu, On the singularity probability of random Bernoulli matrices, *J. Amer. Math. Soc.* **20** (2007), no. 3, 603–628.

[TV10] ———, A sharp inverse Littlewood-Offord theorem, *Random Structures Algorithms* **37** (2010), no. 4, 525–539.

[VE10] A. Venkatesh and J. S. Ellenberg, Statistics of number fields and function fields, *Proceedings of the International Congress of Mathematicians. Volume II* (New Delhi), Hindustan Book Agency, 2010, pp. 383–402.

[Woo14] M. M. Wood, The distribution of sandpile groups of random graphs, *J. Amer. Math. Soc.* **30** (2017), no. 4, 915–958.