LAWS OF COMPOSITION AND ARITHMETIC STATISTICS: FROM GAUSS TO BHARGAVA

ARUL SHANKAR AND XIAOHENG WANG

1. Gauss's law of composition

In his seminal work *Disquisitiones Arithmeticae* of 1801, Karl Friedrich Gass studied the action of $\mathrm{SL}_2(\mathbb{Z})$, the group of integral 2×2 matrices with determinant 1, on the space of integral binary quadratic forms $f(x,y) = ax^2 + bxy + cy^2$ $(a,b,c \in \mathbb{Z})$.[1] The group $\mathrm{SL}_2(\mathbb{Z})$ acts on integral binary quadratic forms by linear substitution of variable as follows:

$$\gamma \cdot f(x,y) = f((x,y) \cdot \gamma)$$

, where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and f is an integral binary quadratic form. This action preserves the *discriminant* $\Delta = b^2 - 4ac$ of binary quadratic forms, i.e., $\Delta(f) = \Delta(\gamma \cdot f)$. Gauss defined a composition law on the orbits for this action: given two integral binary quadratic forms f and g with the same discriminants, Gauss described a method to construct a third integral binary quadratic form $h = f \circ g$, also with the same discriminant. Furthermore, if f' and g' are two integral binary quadratic forms equivalent to f and g respectively under the action of $\mathrm{SL}_2(\mathbb{Z})$, then $f' \circ g'$ is also equivalent to $f \circ g$ under the action of $\mathrm{SL}_2(\mathbb{Z})$. In fact, Gauss proved that the set of $\mathrm{SL}_2(\mathbb{Z})$-orbits on integral binary quadratic forms having a fixed discriminant D form a finite abelian group under composition. We will denote this group by $\mathrm{Cl}(D)$ and the size of $\mathrm{Cl}(D)$ by $h(D)$.

Gauss formulated several conjectures regarding $h(D)$ which have played an enormous part in shaping number theory. The most famous of them is the celebrated class number one conjecture.

Conjecture 1.1 (Gauss). *The list of positive D such that $h(-D) = 1$ is: 3, 4, 7, 8, 11, 19, 43, 67, and 163.*

Conjecture 1.1 has a long and illustrious history which is beautifully detailed by Goldfeld in [23]. It is now a theorem due independently to Baker [1] and Stark [40], [41]. It is worth noting that Heegner [26] had previously published an almost complete proof of Conjecture 1.1, but his paper contained errors and was not

[1] Gauss considered only forms where b is even; however we will follow the modern point of view and allow all three coefficients a, b, and c to be arbitrary integers.

complete. Shortly after the work of Baker and Stark, Deuring [21] filled in the gaps in Heegner's work. Another conjecture regarding $h(D)$ for negative D is the Gauss class number conjecture.

Conjecture 1.2 (Gauss)**.** *The number of positive integers D such that $h(-D)$ is equal to any fixed integer is finite.*

Conjecture 1.2 is a result of the combined work of Hecke [29] (Landau published the theorem, which he attributed to a lecture by Hecke) and Heilbronn [27]. Hecke proves that $h(-D) \to \infty$ as $D \to \infty$ if the generalized Riemann hypothesis is true; Heilbronn proves that $h(-D) \to \infty$ as $D \to \infty$ if the generalized Riemann hypothesis is false! The celebrated result of Siegel [33] provides a rate of growth for $h(-D)$:

Theorem 1.3 (Siegel)**.** *For every $\epsilon > 0$, there exists a constant $c > 0$ such that*

$$h(-D) > cD^{1/2-\epsilon} \tag{1}$$

for every positive integer D.

Siegel proof is ineffective, which is to say that it does not provide a method of computing c given ϵ—only a proof that such a c exists!

Very little is known about the sizes $h(D)$ for positive D. They are expected to behave very differently from the sizes when D is negative. For example, the following is widely believed (though completely unknown).

Conjecture 1.4 (Gauss)**.** *There exist infinitely many positive integers D such that $h(D) = 1$.*

Gauss also made conjectures on the behaviour of $h(D)$ on *average.*

Conjecture 1.5 (Gauss)**.** *For large enough real number X:*

(a) $$\sum_{-X<D<0} h(D) \sim \frac{\pi}{18} \cdot X^{3/2};$$

(b) $$\sum_{0<D<X} h(D) \log \varepsilon_D \sim \frac{\pi^2}{18} \cdot X^{3/2};$$

here $\varepsilon_D = (t + u\sqrt{D})/2$, where t, u are the smallest positive integral solutions of $t^2 - Du^2 = 4$.

It is worth noting that such t, u do not exist if D is negative. Part (a) of Conjecture 1.5 is a result of Mertens [31] and part (b) is a result of Siegel [34]. It is the analogues of these conjectures that we will focus on in this article.

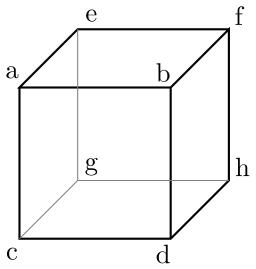
2. Bhargava's laws of composition

In this section, for the sake of convenience, we will restrict ourselves to considering integers D that are *fundamental discriminants*, i.e., integers D such that either $D \equiv 1 \pmod 4$ and is squarefree or $D = 4m$ where $m \equiv 2$ or $3 \pmod 4$ and m is squarefree. For such D, the group $\mathrm{Cl}(D)$ is isomorphic to the *narrow class group* of the quadratic number field $\mathbb{Q}(\sqrt{D})$ and $h(D)$ is the *narrow class number* of $\mathbb{Q}(\sqrt{D})$. This narrow class group is the same as the class group for imaginary quadratic fields (the $D < 0$ case) but can be twice as big for real quadratic fields (the $D > 0$ case). The precise definition of class groups and narrow class groups will not be necessary for us. All number fields have class groups, and these class groups measure the failure of the rings of integers of these number fields to be principle ideal domains.

Narrow class groups of number fields have a naturally occuring abelian group structure and Gauss's law of composition on integral binary quadratic forms having discriminant D corresponds to addition in the narrow class group. Thus, the law of composition can be stated as the following theorem.

Theorem 2.1 (Gauss)**.** *Let $D \neq 0$ be a fundamental discriminant. Then there exists a natural bijection between the set of* $\mathrm{SL}_2(\mathbb{Z})$*-orbits on integral binary quadratic forms with discriminant D and the narrow class group of* $\mathbb{Q}(\sqrt{D})$.

Two centuries after Gauss described his law of composition, Bhargava discovered several new laws of compositions. In what follows, we describe some of them. In our exposition, we closely follow Bhargava's paper [2]. Let $V(\mathbb{Z})$ denote the space $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ of cubes whose vertices are integers. We represent elements of $V(\mathbb{Z})$ as 8-tuples (a, b, c, d, e, f, g, h) viewed as vertices of a cube as follows:



We may slice this cube in three different ways obtaining these three pairs of integral matrices:

$$
\begin{aligned}
M_1 &= \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad N_1 = \begin{bmatrix} e & f \\ g & h \end{bmatrix}, \\
M_2 &= \begin{bmatrix} a & c \\ e & g \end{bmatrix}, \quad N_2 = \begin{bmatrix} b & d \\ f & h \end{bmatrix}, \\
M_3 &= \begin{bmatrix} a & e \\ b & f \end{bmatrix}, \quad N_3 = \begin{bmatrix} c & g \\ d & h \end{bmatrix}.
\end{aligned} \tag{2}
$$

An element $A \in V(\mathbb{Z})$ thus yields three pairs of integral 2×2-matrices (M_i, N_i), $1 \leq i \leq 3$. By considering the discriminant quadratic form

$$Q_i^A := -\det(M_i x - N_i y) \tag{3}$$

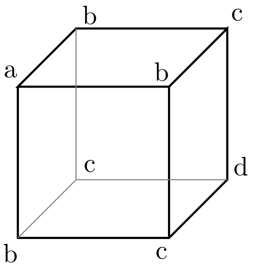
for $1 \leq i \leq 3$, we also obtain three integral binary quadratic forms. Bhargava proves that these three integral binary quadratic forms have the same discriminant! We define the discriminant of A, denoted $\Delta(A)$, to be to this common discriminant of these three binary quadratic forms.

The group $\Gamma = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ acts on $V(\mathbb{Z})$: for $1 \leq i \leq 3$, the i'th component $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ of an element in Γ sends (M_i, N_i) to $(pM_i + qN_i, rM_i + sN_i)$. Furthermore, Γ preserves the discriminant of elements in $V(\mathbb{Z})$. That is, we have $\Delta(A) = \Delta(\gamma \cdot A)$ for $A \in V(\mathbb{Z})$ and $\gamma \in \Gamma$. With Theorem 2.1 as our template to describing laws of composition, we may state Bhargava's first new law of composition.

Theorem 2.2 (Bhargava). *Let $D \neq 0$ be a fundamental discriminant. Then there exists a natural bijection between the set of Γ-orbits on elements in $V(\mathbb{Z})$ with discriminant D and $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{D}))^2$, where $\mathrm{Cl}^+(\mathbb{Q}(\sqrt{D}))$ is the narrow class group of the quadratic field $\mathbb{Q}(\sqrt{D})$.*

The incredible richness of this new composition law is perhaps best described by demonstrating how it gives rise to even more composition laws. First, Bhargava shows that for $A \in V(\mathbb{Z})$ giving rise to the three quadratic forms (3), the sum of Q_1^A, Q_2^A, and Q_3^A, with respect to Gauss composition, is 0. In particular, this law (termed the cube law by Bhargava) is enough to recover all of Gauss composition!

Second, Bhargava shows that the law of composition on integer cubes in $V(\mathbb{Z})$ restricts to *triply symmetric* integer cubes, i.e., those of the form



with $a, b, c, d \in \mathbb{Z}$. These triply symmetric cubes are preserved by the action of $\mathrm{SL}_2(\mathbb{Z})$ embedded diagonally in Γ, and the orbits having fixed fundamental discriminant D form an abelian group under composition. Amazingly, $\mathrm{SL}_2(\mathbb{Z})$-orbits on triply symmetric cubes are in natural bijection with $\mathrm{SL}_2(\mathbb{Z})$-orbits on integral binary cubic forms, whose middle coefficients are multiples of 3: the binary cubic form corresponding to the above triply symmetric integer cube is $ax^2 + 3bx^2y + 3cxy^2 + dy^3$. This leads to another composition law:

Theorem 2.3 (Bhargava). *Let $D \neq 0$ be a fundamental discriminant. Then there exists a natural bijection between the set of $\mathrm{SL}_2(\mathbb{Z})$-orbits on triplicate integral binary cubic forms with discriminant D and $\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))[3]$, where $\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))[3]$ is the 3-torsion subgroup of the class group of the quadratic field $\mathbb{Q}(\sqrt{D})$.*

Details of these and many other composition laws are in the beautiful series of papers [2], [3], [4], [5] by Bhargava.

3. Statistics of number fields

Arithmetic statistics concerns the study of the statistics of arithmetic objects. Two of the foundational questions in the subject are the following.

(1) How are the discriminants of degree-n number fields distributed?
(2) How are the class groups of degree-n number fields distributed?

When $n = 2$, the first question is easy to answer, since an integer D occurs as the discriminant of a quadratic field if and only if D is a fundamental discriminant. Furthermore, each such integer D occurs as the discriminant of exactly one quadratic field. Theorem 2.1 in conjunction with the work of Mertens and Siegel resolving Conjecture 1.5 provides a partial answer to the second question. Siegel in [34] provides a much fuller answer to the second question by computing *all* moments of the sizes of the class groups of number fields. However, even that landmark work does not provide a complete answer. This is because the sizes of class groups do not take into account their group structure. In this regard, the highly influential work of Cohen and Lenstra [17] formulates a detailed series of conjectures that predict the behaviour of class groups of quadratic number fields on average. The most well known of their conjectures is the following:

Conjecture 3.1 (Cohen–Lenstra)**.** *Let p be an odd prime. Then*

(a) *The average size of the p-torsion subgroup in the class group of real quadratic fields is $1 + 1/p$.*

(a) *The average size of the p-torsion subgroup in the class group of imaginary quadratic fields is 2.*

Their conjecture goes much further and in fact predicts the distribution of class groups of quadratic number fields. Very little is proved of their conjecture. The only known case is that of $p = 3$, which is due to Davenport and Heilbronn in work that predates the conjecture of Cohen and Lenstra.

Theorem 3.2 (Davenport–Heilbronn)**.** *We have*

(a) *The average size of the 3-torsion subgroup in the class group of real quadratic fields is 4/3.*

(a) *The average size of the 3-torsion subgroup in the class group of imaginary quadratic fields is 2.*

When $n \geq 3$, very little is known of either of the two questions posed in the beginning of this section. Before the work of Bhargava, the only complete result in this regard was the following theorem of Davenport and Heilbronn [20].

Theorem 3.3 (Davenport–Heilbronn)**.** *Let $N_3(\xi, \eta)$ denote the number of cubic fields K, up to isomorphism, that satisfy $\xi < \mathrm{Disc}(K) < \eta$. Then*

$$\begin{aligned} N_3(0, X) &= \frac{1}{12\zeta(3)} X + o(X); \\ N_3(-X, 0) &= \frac{1}{4\zeta(3)} X + o(X), \end{aligned} \tag{4}$$

where ζ denotes the Riemann-Zeta function.

As far as the second question is concerned, the Cohen–Lenstra heuristics have been modified by Cohen and Martinet [18] to obtain conjectures for higher degree number fields. Before the work of Bhargava (described in the next section), no case of this conjecture had been proven.

4. Bhargava's advances in Arithmetic Statistics

Davenport, using geometry-of-numbers techniques, proved the following theorem [19] which was a key input in Theorems 3.2 and 3.3.

Theorem 4.1 (Davenport)**.** *Let $N(\xi, \eta)$ denote the number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of irreducible integer-coefficient binary cubic forms f satisfying $\xi < \mathrm{Disc}(f) < \eta$. Then*

$$N(0, X) = \frac{\pi^2}{72} \cdot X + O(X^{15/16})\,; \; N(-X, 0) = \frac{\pi^2}{24} \cdot X + O(X^{15/16})\,.$$

This furthers the works of Siegel and Mertens resolving Conjecture 1.5 by counting $\mathrm{SL}_2(\mathbb{Z})$-orbits on integral binary quadratic forms. It had previously been understood through works of [42] that the statistics of quartic fields can be studied via the representation of $G_4 = \mathrm{GL}_2 \times \mathrm{SL}_3$ on the space $W_4 = (\mathrm{Sym}^2\mathbb{Z}^3 \otimes \mathbb{Z}^2)^*$ of pairs of ternary quadratic forms. However, two major obstacles remained: first, though the rational orbits for the action of $G_4(\mathbb{Q})$ on $W_4(\mathbb{Q})$ were understood to correspond to quartic extensions of $\mathbb{Q}$, there was no corresponding interpretation of the integral orbits of $G_4(\mathbb{Z})$ acting on $W_4(\mathbb{Z})$. Second, the combinatorial difficulties in counting $\mathrm{SL}_2(\mathbb{Z})$-orbits on the space of integral binary quadratic forms (a 2-dimensional space) and in counting $\mathrm{GL}_2(\mathbb{Z})$-orbits on the space of integral binary cubic forms (a 3-dimensional space) grow infinitely when dealing with $G_4(\mathbb{Z})$-orbits on $W_4(\mathbb{Z})$ which is 12-dimensional!

The first difficulty was resolved by Bhargava in [4], where he proves the following remarkable theorem.

Theorem 4.2 (Bhargava)**.** *There is a canonical bijection between the set of* $\mathrm{GL}_2(\mathbb{Z})\times \mathrm{SL}_3(\mathbb{Z})$*-orbits on the space* $(\mathrm{Sym}^2\mathbb{Z}^3 \otimes \mathbb{Z}^2)^*$ *of pairs of integral ternary quadratic forms and the set of ismorphism classes of pairs* (Q, R)*, where* Q *is a quartic ring and* R *is a cubic resolvent ring of* Q*.*

It is important to note that a very slightly modified representation is shown by Bhargava to yield another important law of composition.

Theorem 4.3 (Bhargava)**.** *There is a bijection between the set of* $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$*-orbits on the space* $\mathrm{Sym}^2\mathbb{Z}^3 \otimes \mathbb{Z}^2$ *and the set of equivalence classes of triples* (R, I, δ)*, where* R *is a nondegenerate cubic ring over* $\mathbb{Z}$*,* I *is an ideal of* R *having rank* 3 *as a* $\mathbb{Z}$*-module, and* δ *is an invertible element of* $R \otimes \mathbb{Q}$ *such that* $I^2 \subset (\delta)$ *and* $N(I)^2 = N(\delta)$*.*

Introducing fundamental new tools, Bhargava transformed the reach of the geometry-of-numbers methods used by Mertens, Siegel, and Davenport. These new tools made it possible to resolve enormous combinatorial difficulties and determine asymptotics for the number of absolutely irreducible $G_4(\mathbb{Z})$-orbtis on $W_4(\mathbb{Z})$, where an orbit is said to be *absolutely irreducible* if it corresponds to a quartic integral domain R such that the Galois closure of the fraction field of R over $\mathbb{Q}$ is S_4. This led to the following results proved in [6].

Theorem 4.4 (Bhargava)**.** *Let* $N_4^{(i)}(\xi, \eta)$ (*resp.* $M_4^{(i)}(X)$) *denote the number of* S_4*-quartic fields* K (*resp. quartic orders* $\mathcal{O}$ *contained in* S_4*-quartic fields*) *having* $4 - 2i$ *real embeddings such that* $|\mathrm{Disc}(\mathcal{O})| < X$*. Then*

(a) $\displaystyle\lim_{X\to\infty} \frac{N_4(X)}{X} = \frac{1}{n_i}\frac{\zeta(2)^2\zeta(3)}{\zeta(5)},$

(a) $\lim_{X\to\infty} \dfrac{M_4(X)}{X} = \dfrac{1}{n_i}\prod_p (1+p^{-2}-p^{-3}-p^{-4}),$

where $n_0 = 48$, $n_1 = 8$, *and* $n_2 = 16$.

These methods in conjunction with Theorem 4.3 also lead to the following theorem, which is the first, and thus far only, result proving an instance of the Cohen-Lenstra-Martinet heuristics involving fields having degree greater than 2.

Theorem 4.5 (Bhargava)**.** *We have*

(a) *The average size of the* 3*-torsion subgroup in the class group of cubic fields having positive discriminants is* $5/4$.

(a) *The average size of the* 3*-torsion subgroup in the class group of cubic fields having negative discriminants is* $3/2$.

Quintic fields had been known to correspond to $G_5(\mathbb{Q})$-orbits on $W_5(\mathbb{Q})$, where $G_5 = \mathrm{GL}_4 \times \mathrm{SL}_5$ and W_5 is the space of 4-tuples of 5×5-altering forms. The space W_5 is 50-dimensional, which is a large increase over the 12-dimensional space W_4. The combinatorial difficulties, both in understanding what the integral orbits parameterize and in counting the integral orbits, are correspondingly larger. However, Bhargava resolves them both in [5] and [7], respectively, yielding the following theorems.

Theorem 4.6 (Bhargava)**.** *There is a canonical bijection between the* $\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$*-orbits on the space* $\mathbb{Z}^4 \otimes \wedge^2\mathbb{Z}^5$ *of quadruples of* 5×5 *skew-symmetric matrices and the set of isomorphism classes of pairs* (R, S)*, where* R *si a quintic ring and* S *is a sextic resolvent of* R*.*

Theorem 4.7 (Bhargava)**.** *Let* $N_5^{(i)}(\xi,\eta)$ (*resp.* $M_5^{(i)}(X)$) *denote the number of quintic fields* K (*resp. quintic orders* $\mathcal{O}$ *contained in quintic fields*) *having* $4-2i$ *real embeddings such that* $|\mathrm{Disc}(\mathcal{O})| < X$*. Then*

(a) $\lim_{X\to\infty} \dfrac{N_5(X)}{X} = \dfrac{1}{n_i}\prod_p (1+p^{-2}-p^{-4}-p^{-5},$

(a) $\lim_{X\to\infty} \dfrac{M_4(X)}{X} = \dfrac{\alpha}{n_i},$

where

$$\alpha = \prod_p \Big(\frac{p-1}{p} \sum_{[R_p:\mathbb{Z}_p]=5} \frac{1}{|\mathrm{Aut}_{\mathbb{Z}_p}(R_p)|}\cdot\frac{1}{\mathrm{Disc}_p(R_p)}\Big),$$

$n_0 = 240$, $n_1 = 24$, *and* $n_2 = 16$.

5. Elliptic curves

An elliptic curve E over $\mathbb{Q}$ is given by the equation

$$E : y^2 = x^3 + Ax + B, \tag{5}$$

where the discriminant $-(4A^3 + 27B^2)$ is nonzero. The rational points $E(\mathbb{Q})$ of an elliptic curve, along with the point at infinity, form an abelian group. The following famous result is due to Mordell:

Theorem 5.1 (Mordell)**.** *The group $E(\mathbb{Q})$ is finitely generated as an abelian group.*

This implies that we have the isomorphism

$$E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r,$$

where T is a finite abelian group and r is denoted the *rank* of E. The following remarkable result of Mazur [30] gives all the possibilities for the group T.

Theorem 5.2 (Mazur)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then the torsion subgroup T of $E(\mathbb{Q})$ can only be $\mathbb{Z}/n\mathbb{Z}$ for $1 \leq n \leq 12$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ for $m = 2, 4, 6$ or 8.*

The rank r, on the other hand, is much less understood. Given an elliptic curve E over $\mathbb{Q}$, it is possible to associate an L-function to it. These L-functions have many of the same features as the Riemann zeta function. They have Euler products, functional equations, and a meromorphic continuation to the entire complex plane. We will normalize these L-functions so that the line of symmetry of their functional equation is $\mathrm{Re}(s) = 1$. The form of these functional equations is the following.

$$\Lambda(E, s) = \omega(E)N^{1-s}\Lambda(E, 2 - s), \tag{6}$$

where Λ is the completed L-function of E, N is the conductor of E, and $\omega(E)$ is the root number of E. The precise definitions of Λ, N, and $\omega(E)$ will not be important to us. However, it is important to note that $\omega(E)$ is ± 1. The order of the zero of L (equivalently the zero of Λ) at $s = 0$ is called the *analytic rank* of E. Then the Birch–Swinnerton-Dyer conjecture is the following:

Conjecture 5.3 (Birch–Swinnerton-Dyer)**.** *The rank of an elliptic curve E is equal to the analytic rank of E.*

The parity of the analytic rank of E is determined by the root number; the analytic rank is even or odd depending on whether $\omega(E)$ is 1 or -1, respectively. Thus, the Birch–Swinnerton-Dyer conjecture implies that the parity of the rank of E is determined by $r(E)$.

It is widely believed (though yet unproven) that $r(E)$ is 1 half the time and -1 half the time. Together with the Birch–Swinnerton-Dyer conjecture, this would imply that the rank is even half the time and odd half the time. In conjunction with a general belief that elliptic curves should have as few rational points as they can get away with, with have the following "minimalist" conjecture due to Goldfeld and Katz–Sarnak.

Conjecture 5.4 (Goldfeld, Katz–Sarnak). *The average rank of elliptic curves is* $1/2$*. The proportion of elliptic curves having rank* 0 *is* 50%*; the proportion having rank* 1 *is* 50%*.*

There are two important points to make regarding the above conjecture. The first is that the believed 0% of elliptic curves having rank greater than or equal to 2 still constitutes infinitely many curves! The second is that statements about the average rank of elliptic curves, or statements concerning proportions of elliptic curves cannot be made precisely without first ordering elliptic curves in some way. This can be done in several natural ways: we may order elliptic curves by conductor or discriminant or some sort of height. Note the elliptic curve $E_{A,B} : y^2 = x^3+Ax+B$ is isomorphic to the elliptic curve $E_{u^4A,u^6B} : y^2 = x^3+u^4Ax+u^6B$ under the map $(x,y) \mapsto (u^2x, u^3y)$ for any rational number u and we certainly do not want to count both. Hence we may scale A, B so that they are both integers and that there is no prime p such that $p^4 \mid A$ and $p^6 \mid B$. Because of this apparent "weight" of A and B (which will appear again in the definition of the height for hyperelliptic curves in the next section), we define the "naive" height of an elliptic curve $E_{A,B}$ to be

$$H(E_{A,B}) = \max\{4A^3, 27B^2\}. \tag{7}$$

The extra factors of 4 and 27 are there to balance their contribution to the discriminant and have no effect on the average behavior.

Conditional on the generalized Riemann hypothesis, Brumer [16] showed that the average analytic rank of elliptic curves, when ordered by height, is finite and bounded by 2.3. Still assuming the generalized Riemann hypothesis, this constant was improved by 2 and 1.79 by Heath-Brown [25] and Young [43], respectively. However, no unconditional results were proven about the finiteness of the average analytic rank (or the average rank) of elliptic curves.

The geometry-of-numbers methods developed by Bhargava may be applied to the following representations that are intimately connected to ranks of elliptic curves:

$$\begin{array}{ccc} \mathrm{GL}_2(\mathbb{Z}) & \to & \mathrm{End}(\mathrm{Sym}^4(\mathbb{Z}^2)) \\ \mathrm{GL}_3(\mathbb{Z}) & \to & \mathrm{End}(\mathrm{Sym}^3(\mathbb{Z}^3)) \\ \mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_4(\mathbb{Z}) & \to & \mathrm{End}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2(\mathbb{Z}^4)) \\ \mathrm{GL}_5(\mathbb{Z}) \times \mathrm{GL}_5(\mathbb{Z}) & \to & \mathrm{End}(\mathbb{Z}^5 \otimes \wedge^2(\mathbb{Z}^5)). \end{array}$$

In joint work with the first named author, this yielded the following theorem, which was a result of a series of papers [11], [12], [13], [14].

Theorem 5.5. *When elliptic curves over* $\mathbb{Q}$ *are ordered by height, their average rank is* $< .885$*; a density of at least* 83.75% *have rank* 0 *or* 1*; a density of at least* 20.62% *have rank* 0*.*

Extending these methods still further, and using the famous Gross–Zagier formula [24], Kolyvagin's theory of Euler systems [28], and recent works of Dokchitser–Dockchitser [22] and recent Skinner, Urban, and Zhang [35], [36], [37], [38], [39], Bhargava, Skinner, and Zhang obtain the following stunning result [15].

Theorem 5.6. *When elliptic curves over $\mathbb{Q}$ are ordered by height, at least* 66.48% *of them satisfy the Birch–Swinnerton-Dyer conjecture; at least* 16.50% *of elliptic curves over $\mathbb{Q}$ have algebraic and analytic rank zero; at least* 20.68% *have algebraic and analytic rank one.*

6. Hyperelliptic curves

Finally, we consider hyperelliptic curves, i.e., (projective) curves defined by an equation of the form

$$y^2 = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n, \tag{8}$$

where the polynomial on the right hand side is assumed to have no repeated factors. The genus of the above curve where $n = 2g+1$ or $2g+2$ is g and so when $n \geq 2$ these curves have genus at least 2. Curves having genus 0 have either no rational points or infinitely many rational points all of which can be parameterized algebraically using one parameter just like the parametrization of Pythagorean triples. Curves of genus 1 can have no rational points. When they do have rational points, they are elliptic curves and as we have seen in the previous section, they can have finitely many rational points (when $r = 0$), or infinitely many rational points (when $r \geq 1$). Curves with genus 2 or higher are addressed by a tremendously powerful theorem of Faltings (originally a conjecture of Mordell):

Theorem 6.1 (Faltings)**.** *When $n \geq 5$, equation* (8) *has finitely many rational solutions.*

However, the above theorem does not address the question of *how many* points $C(\mathbb{Q})$ has. In fact, Theorem 6.1 is ineffective, and does not provide any bound on the size of $C(\mathbb{Q})$. Effectivising Theorem 6.1 is open and would be a major breakthrough, but we can apply the philosophy of Arithmetic Statistics and ask instead: what is the average number of rational points in families of curves having genus $g \geq 2$. In this regard, there have been a slew of recent results, many of which crucially use Bhargava's methods. We describe three of these results below.

First, we consider the family of monic odd hyperelliptic curves, i.e., curves cut out by the equation (8) with $a_0 = 1$ and n odd. Each such curve has at least one rational point (the point at infinity). We order these curves C by height which is defined as follows:

$$H(C) = \max\{|a_1|, |a_2|^{1/2}, \ldots, |a_n|^{1/n}\}. \tag{9}$$

In [9], Bhargava and Gross study the Selmer groups of Jacobians of these curves, and using their results Poonen and Stoll prove the following result in [32].

Theorem 6.2 (Poonen–Stoll)**.** *For each odd $n \geq 7$, a positive proportion of curves in the family of monic degree-n hyperelliptic curves, when ordered by height, have exactly one rational point. Furthermore, this proportion tends to* 1 *as n tends to infinity.*

Next we consider the family of even hyperelliptic curves, i.e., curves C cut out by (8) with even $n \geq 6$. We order curves in this family by the following height:

$$H(C) = max\{|a_i|\}.$$

Bhargava proves the following result in [8]:

Theorem 6.3. *For each even $n \geq 8$, a positive proportion of curves in the family of degree-n hyperelliptic curves, when ordered by height, have no rational points. Furthermore, this proportion tends to* 1 *as n tends to infinity.*

Finally, in [10], Bhargava, Gross, and Wang prove the following stunning results.

Theorem 6.4. *For any even $n \geq 2$, a positive proportion of curves in the family of degree-n hyperelliptic curves, when ordered by height, have no points over any odd degree extension of $\mathbb{Q}$.*

Theorem 6.5. *Fix any $m > 0$. Then as $n \to \infty$, a proportion approaching* 1 *of degree-n hyperelliptic curves have no points defined over any extension of $\mathbb{Q}$ having odd degree $\leq m$.*

References

[1] A. Baker, Imaginary quadratic fields with class number 2, *Annals of Math.* (2) **94** (1971), 139–152.

[2] M. Bhargava, Higher composition laws I: A new view on Gauss composition, and quadratic generalizations, *Ann. of Math.* **159** (2004), no. 1, 217–250.

[3] M. Bhargava, Higher composition laws. II. On cubic analogues of Gauss composition. *Ann. of Math. (2)* **159** (2004), no. 2, 865–886.

[4] M. Bhargava, Higher composition laws III: The parametrization of quartic rings, *Ann. of Math.* **159** (2004) 1329–1360.

[5] M. Bhargava, Higher composition laws. IV. The parametrization of quintic rings. *Ann. of Math. (2)* **167** (2008), no. 1, 53–94.

[6] M. Bhargava, The density of discriminants of quartic rings and fields. *Ann. of Math. (2)* **162** (2005), no. 2, 1031–1063.

[7] M. Bhargava, The density of discriminants of quintic rings and fields, *Ann. of Math. (2)* **172** (2010), no. 3, 1559–1591.

[8] M. Bhargava Most hyperelliptic curves over Q have no rational points, http://arxiv.org/abs/1308.0395.

[9] M. Bhargava and B. H. Gross, The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point, *Automorphic representations and L-functions, Tata Inst. Fundam. Res. Stud. Math.* , **22**, Tata Inst. Fund. Res., Mumbai, (2013), 23–91.

[10] M. Bhargava, B. H. Gross, and X. Wang, Pencils of quadrics and the arithmetic of hyperelliptic curves, http://arxiv.org/abs/1310.7692.

[11] M. Bhargava and A. Shankar, Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves, *Ann. of Math. (2)* **181** (2015), no. 1, 191–242.

[12] M. Bhargava and A. Shankar, Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0, *Ann. of Math. (2)* **181** (2015), no. 2, 587–621.

[13] M. Bhargava and A. Shankar, The average number of elements in the 4-Selmer groups of elliptic curves is 7, http://arxiv.org/abs/1312.7333

[14] M. Bhargava and A. Shankar, The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1, http://arxiv.org/abs/1312.7859

[15] M. Bhargava, C. Skinner, and W. Zhang, A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture, http://arxiv.org/pdf/1407.1826v2.pdf.

[16] A. Brumer, The average rank of elliptic curves. I. *Invent. Math.* **109** (1992), no. 3, 445–472.

[17] H. Cohen and H. W. Lenstra, Heuristics on class groups of number fields, Number theory (Noordwijkerhout, 1983), 33–62, *Lecture Notes in Math.* **1068**, Springer, Berlin, 1984.

[18] H. Cohen and J. Martinet, Étude heuristique des groupes de classes des corps de nombres, *J. Reine Angew. Math.* **404** (1990), 39–76.

[19] H. Davenport, On the class number of binary cubic forms I and II, *J. London Math. Soc.* **26** (1951), 183–198.

[20] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, *Proc. Roy. Soc. London Ser. A* **322** (1971), no. 1551, 405–420.

[21] M. Deuring, Imaginare quadratische Zahlkorper mit der Klassenzahl Eins, *Invent. Math.* **5** (1968), 169-179.

[22] T. Dokchitser and V. Dokchitser, On the Birch–Swinnerton-Dyer quotients modulo squares, *Ann. of Math. (2)* **172** (2010), no. 1, 567–596.

[23] D. Goldfeld, The Gauss class number problem for imaginary quadratic fields, *Bull. Amer. Math. Soc. (N.S.)* **13** (1985), no. 1, 23–37.

[24] B. H. Gross and D. Zagier, Heegner points and derivatives of L-series, *Invent. Math.* **84** (1986), no. 2, 225–320.

[25] D. R. Heath-Brown, The average analytic rank of elliptic curves. *Duke Math. J.* **122** (2004), no. 3, 591–623.

[26] K. Heegner, Diophantische Analysis und Modulfunktionen, *Math. Z.* **56** (1952), 227–253.

[27] H. Heilbronn, On the class number in imaginary quadratic fields, *Quart. J. Math. Oxford Ser. 2* **5** (1934), 150–160

[28] V. A. Kolyvagin, Euler Systems, *The Grothendieck Festschrift*, Progr. in Math. **87**, Birkhauser Boston, Boston, MA (1990).

[29] E. Landau, Uber die Klassenzahl imaginar-quadratischer Zahlkorper, *Gottinger Nachr.* (1918), 285–295.

[30] B. Mazur, Modular curves and the Eisenstein ideal, *Publications Mathmatiques de l'IHS (1)* **47** 33–186.

[31] F. Mertens, Ueber einige asymptotische Gesetze der Zahlentheorie, *J. reine angew Math.* **77** (1874), 289–338.

[32] B. Poonen and M. Stoll, Most odd degree hyperelliptic curves have only one rational point, *Ann. of Math. (2)* **180** (2014), no. 3, 1137–1166.

[33] C. L. Siegel, Uber die Classenzahl quadratischer Zahlkorper, *Acta Arith.* **1** (1935), 83-86.

[34] C. L. Siegel, The average measure of quadratic forms with given determinant and signature, *Ann. of Math. (2)* **45** (1944), 667–685.

[35] C. Skinner, A converse to a theorem of Gross–Zagier–Kolyvagin, http://arxiv.org/abs/1405.7294

[36] C. Skinner, Multiplicative reduction and the cyclotomic main conjecture for modular forms, http://arxiv.org/abs/1407.1093.

[37] C. Skinner and E. Urban, The Iwasawa main conjectures for GL(2), *Invent. Math.*, **195** (2014), no. 1, 1–277.

[38] C. Skinner and E. Urban, forthcoming.

[39] C. Skinner and W. Zhang, Indivisibility of Heegner points in the multiplicative case, http://arxiv.org/abs/1407.1099.

[40] H. Stark, A complete determination of the complex quadratic fields of class number one, *Mich. Math. J.* **14** (1967),1–27.

[41] H. Stark, A transcendence theorem for class number problems I, II, *Annals of Math.* (2) **94** (1971), 153–173; *ibid.* **96** (1972), 174–209.

[42] D. Wright and A. Yukie, Prehomogeneous vector spaces and field extensions, *Invent. Math.* **110** (1992), no. 2, 283–314.

[43] M. P. Young, Low-lying zeros of families of elliptic curves. *J. Amer. Math. Soc.* **19** (2006), no. 1, 205–250.