ON CLASS NUMBERS AS DETERMINANTS OF RANDOM MATRICES

A Thesis
Submitted to the Faculty of Mathematics
by

PRAJEET BAJPAI

Dartmouth College
Hanover, New Hampshire

MAY 2016

Advisor:

JOHN VOIGHT

ABSTRACT

In this thesis, we propose a heuristic model for class groups (and regulators) of quadratic number fields, which is then experimentally verified. In the imaginary quadratic case, we model the class group as the cokernel of a random integer matrix. This in turn suggests that the $\log$ of the class numbers (which are then the determinants of such matrices) is normally distributed. We also provide related heuristics for the real quadratic case that allow us to make independent predictions for the class number and the regulator.

Acknowledgements

First of all I would like to thank my advisor, Professor John Voight, for making this senior thesis possible and for his help, support and guidance throughout the duration of its execution. Additionally, I would like to thank Melanie Matchett Wood for her assistance with the project, including but not limited to the helpful suggestion that we consider the naturalized class group for *all* fundamental discriminants, rather than fixing the number of prime divisors of the discriminant.

Finally I would also like to thank the Mathematics Department at Dartmouth College, and the incredible professors I had the opportunity to meet and study with, for providing me with a unique and enriching mathematical experience during my years here as an undergraduate.

Contents

Chapter 1

Introduction

This chapter outlines some basic terms, and then presents our heuristic model for imaginary quadratic fields. Experimental and theoretical support for the model is provided in subsequent chapters.

1.1 Basic Definitions

A number field is a finite extension of the field of rational numbers. For example, consider quadratic fields, i.e. fields of the form $\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}$ for an integer m which is not a perfect square. In this thesis, we are concerned precisely with quadratic fields. We will discuss both the imaginary and real quadratic case, and see why they must be dealt with somewhat independently.

Every number field contains a subring, known as the ring of integers, which consists of the algebraic integers in the field: an *algebraic integer* is a complex number that is a root of a monic polynomial with coefficients in $\mathbb{Z}$

For an algebraic integer α, the monic irreducible polynomial over $\mathbb{Q}$ that has α as a root actually has coefficients in $\mathbb{Z}$. Therefore, the polynomial mentioned in the definition above is in fact the minimal polynomial of the algebraic integer.

The ring of integers is different from $\mathbb{Z}$ but still has the property that ideals in the subring

factor uniquely into prime ideals. Let us denote the ring of integers of a number field K as $\mathbb{Z}_K$. For the case of quadratic fields $K = \mathbb{Q}(\sqrt{m})$ for squarefree m, $\mathbb{Z}_K$ is easy to describe. It is:

$$\{a + b\sqrt{m} : a, b \in \mathbb{Z}\} \text{ if } m = 2 \text{ or } 3 \pmod 4$$
$$\{\tfrac{a+b\sqrt{m}}{2} : a, b, \in \mathbb{Z}\} \text{ if } m = 1 \pmod 4$$

An integer D is a fundamental discriminant if it is not equal to 1, not divisible by the square of any odd prime, and for which one of the following is true: either $D \equiv 1 \mod 4$ or $\frac{D}{4} \equiv 2, 3 \mod 4$. Quadratic number fields can be ordered by fundamental discriminants such that every field appears exactly once.

$\mathbb{Z}[i] \subseteq \mathbb{Q}(i)$ is a Euclidean domain, but $\mathbb{Z}[\sqrt{-5}]$ is not even a unique factorization domain since $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. We might seek to measure how far a given number field is from satisfying unique factorisation of elements in its ring of integers (we already know ideals in it factor uniquely into primes). To do this, we construct the **ideal class group** of the number field, which measures how far ideals in the field are from being principal, or rather how many distinct *classes* of non-principal ideals there are.

The set of ideals in a number field do not in themselves form a group. In order to create a group structure, we consider instead the *fractional ideals*:

Let K be a number field with ring of integers $\mathbb{Z}_K$. A subset $\mathfrak{a} \subseteq K$ is called a fractional ideal if there exists $\alpha \in K^\times$ such that $\alpha\mathfrak{a} \subseteq \mathbb{Z}_K$ is an ideal of $\mathbb{Z}_K$. Every fractional ideal has an inverse $\mathfrak{a}^{-1}$, a fractional ideal such that $\mathfrak{a}\mathfrak{a}^{-1} = \mathbb{Z}_K$. Thus, this set has the structure of a finite abelian group under ideal multiplication.

We take the group I_K of fractional ideals modulo the subgroup P_K of principal fractional ideals. The resulting quotient is known as the **class group** of the number field, denoted $\mathrm{Cl}(K)$. For more details on the construction and working of the class group, see Marcus [1] or Cox [2].

It is a basic but important result in algebraic number theory that the class group is always a finite abelian group, and we shall see one proof of this due to Minkowski in the

chapter on factor bases. The order of the class group is known as the **class number**. The class number of a quadratic field $\mathbb{Q}[\sqrt{D}]$ is commonly denoted $h(D)$, suggesting one can look at it as a map $h : \mathbb{Z} \to \mathbb{Z}^+$.

1.2 The Structure of the Class Group

What do we know about class groups and class numbers? The Brauer-Siegel theorem [3][4] tells us that at least for imaginary quadratic fields the class number tends to infinity with $|D|$.

Theorem 1.2.1 (Brauer-Siegel) *Let $D < 0$ range over negative fundamental discriminants. Then we have:*

$$\lim_{D \to -\infty} \frac{\log h(D)}{\log |D|} = \frac{1}{2}$$

Put another way, the $\log(h(D))$ tends asymptotically to $\log \sqrt{|D|}$. A similar result is available for the real quadratic case, but it requires an extra term which we will come to later.

What about the structure of the class group? For cases where $h(D) = 9$, how often do we see $\mathbb{Z}/9\mathbb{Z}$ as compared to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$? How are class numbers distributed? Various results about class groups have been proven in recent decades, but much about the structure of class groups remains a mystery. About the only concrete thing we know on these groups comes from Gauss. Gauss's Genus Theory tells us the precise description for $\mathrm{Cl}(K)[2]$, the 2-torsion subgroup of the class group of a number field K. This is the subgroup of elements that square to the identity. Specifically it tells us that for $K = \mathbb{Q}[\sqrt{D}]$, we have $\mathrm{Cl}(K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{\omega(D)-1}$, where $\omega(D)$ is the number of prime divisors of D.

Since we have a clear theoretical description for $\mathrm{Cl}(K)[2]$, it is useful here to consider the group $\mathrm{Cl}(K)/\mathrm{Cl}(K)[2]$. This is the part of the class group that we wish to model using random integer matrices. In this thesis, we will refer to $\mathrm{Cl}(K)/\mathrm{Cl}(K)[2]$ as the *naturalized*

class group $\mathrm{Cl}^\natural(K)$ of K, and denote its order as the *naturalized class number* $h^\natural$. We shall discuss more precise implications of this structure in Chapter 3.

1.3 Regulators and Real Quadratic Fields

In imaginary quadratic fields other than $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$, the only units are roots of unity. For real quadratics, in addition to 1 and -1, there is an additional group of units that we know to be infinite cyclic by Dirichlet's Unit Theorem. The smallest $\epsilon > 1$ that generates this group of units is known as the **fundamental unit**. For $\mathbb{Z}[\sqrt{2}]$, we have $\epsilon = 1 + \sqrt{2}$. Often, though, it is much larger: Marcus [1] tells us for $\mathbb{Z}[\sqrt{31}]$ it is $1520 + 273\sqrt{31}$, and even more surprisingly for $\mathbb{Z}[\sqrt{94}]$ it is $2143295 + 221064\sqrt{94}$. For $\mathbb{Z}[\sqrt{95}]$ it is $39 + 4\sqrt{95}$. Since the fundamental unit is uniquely determined, the **regulator** of a number field can be defined as $\log|\epsilon|$, where ϵ is the fundamental unit.

The regulator encodes certain non-trivial information about the real quadratic field. For real quadratic fields, we find that the class number is typically small, although it is not known whether it is 1 for infinitely many cases. In comparison the regulator (as evidenced above) can be surprisingly large. The Brauer-Siegel Theorem in the real quadratic case tells us that

$$\lim_{D \to -\infty} \frac{\log(h(D)R(D))}{\log|D|} = \frac{1}{2}$$

. If the class number stays small, we can expect the regulator to grow with increasing D. We might also expect the distribution of $\log(hR)$ in the real case to match that of $\log h$ in the imaginary case. Data on this is presented in the final chapter on real quadratic fields.

1.4 Heuristic Model for Imaginary Quadratics

Cohen and Lenstra [5] give us a heuristic for the distribution of class groups, especially the odd part of the class group, that comes from considering how random abelian groups

might behave. The Cohen-Lenstra heuristics predict that a particular random abelian group appears with probability inversely proportional to its number of automorphisms.

So consider again the example of groups of order 9, $\mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$. We know that $\mathrm{Aut}(\mathbb{Z}/9\mathbb{Z}) \cong (\mathbb{Z}/9\mathbb{Z})^\times$ and $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. Thus we expect to see $\mathbb{Z}/9\mathbb{Z}$ more more often than $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, with a ratio of $[8:1]$ in inverse proportion to their number of automorphisms.

Given the dearth of predictive results on class groups, heuristic models are extremely important for providing insight into what these abelian groups look like and how they behave. This thesis hopes to extend the results taken modulo a number of primes and see if it can be done all at once, so that class groups may be related directly to cokernels of random integer matrices. It offers some experimental results on how one can make class groups look like random matrices, considers what parameters on the size of the matrix and its entries are useful, and suggests that studying the behaviour of random matrices can give us insight into the functioning of these rather mysterious groups.

To model class groups of imaginary quadratic fields, we propose the following heuristic.

Model 1.4.1 *For an imaginary quadratic field $K = \mathbb{Q}(\sqrt{D}), |D| \to \infty$, we model the class group $\mathrm{Cl}(D)$ as follows:*
Let $n(D)$ and $X(D)$ be such that

$$n(D) \text{ is an integer of size } (\log\log|D|^{1/2})^{O(1)}$$

$$\sqrt{n(D)}X(D) \to \left(\frac{D^{\frac{1}{2}}}{2^{\log\log|D|}}\right)^{\frac{1}{n}}$$

Let A_n be an $n(D) \times n(D)$ integer matrix whose elements are drawn from a gaussian distribution of mean 0 and variance $(X(D))^2$. Then $\mathrm{Cl}^\natural(K)$ is modelled by $\mathrm{coker}\, A_n$, and $h^\natural(D)$ by $|\det A_n|$.

Combining this with results about the determinants of random matrices suggests that

$\log h^\natural(D)$ is distributed normally with mean $= \log|D|^{\frac{1}{2}} - \log 2 \log\log|D|$ and variance $= (\log\log\log|D|^{\frac{1}{2}})^{O(1)}$. Chapters 3 and 5 motivate these expressions for the mean and variance. In Chapter 6, we will present a variant of this model for real quadratic fields $(D > 0)$.

We see that $n(D)$ grows quite slowly with respect to D, and as a result we see $X(D)$ growing at a much faster rate. This is in accordance with the Cohen-Lenstra heuristics, which predict that the class group is generally found as the direct product of a small number of cyclic subgroups. The discussion in Chapter 4 makes clearer the connection between $n(D)$ and this direct product.

In chapter 2 we present experimental data (for the imaginary quadratic case) on naturalized class groups and random matrices, which are in accordance with our conjectures. In chapter 3, we discuss theoretical results that allow us to postulate a mean and variance for $h^\natural$. The Brauer-Siegel theorem and predictions from Genus Theory suggest the expression for the mean, and the Analytic Class Number formula gives us the next order term that indicates what the variance looks like. In Chapter 5 we consider results in random matrix theory, and see that $n(D) \to \log\log|D|^{\frac{1}{2}}$ appears as the most appropriate way to link matrices and class groups together. The plausibility of this expression for $n(D)$ is experimentally verified. The somewhat more involved expression for $X(D)$ is derived from that for $n(D)$ and the requirement that the means for random matrices and naturalized class groups align. At the end of Chapter 5, we combine the results from genus theory, the Analytic Class Number formula, and random matrix theory to present calculations that support our model.

Chapter 2

Data on Class Numbers for Imaginary Quadratic Fields

In this this chapter, we consider the imaginary quadratic case and present some data. We compare the distribution of naturalized class numbers to the distribution of $\log|\det|$ of appropriately sized matrices and see how they relate, and also verify that the expressions for $n(D)$ and $X(D)$ are experimentally valid.

2.1 Approach

In the imaginary case there are no nontrivial units or regulators to worry about, so we just sample class numbers at various orders of magnitude of fundamental discriminant and consider their distributions. We took 10000 randomly sampled fundamental discriminants (with replacement) in the range $[0, D_0]$, with $D_0 = -10^k$ for integers k between 5 and 24. For each sample point we then computed the class number. Using the theorem that $\#\operatorname{Cl}(K)[2] = 2^{\omega(D)-1}$, we divided the class number by $2^{\omega(D)-1}$ to cancel out the contribution from Genus Theory. Recall that we named the resulting quantity the 'naturalized class number', $h^\natural$.

Finally, we checked the distribution of $\log h^\natural(D)$ for $D \in [D_0, 0]$ for each choice of D_0.

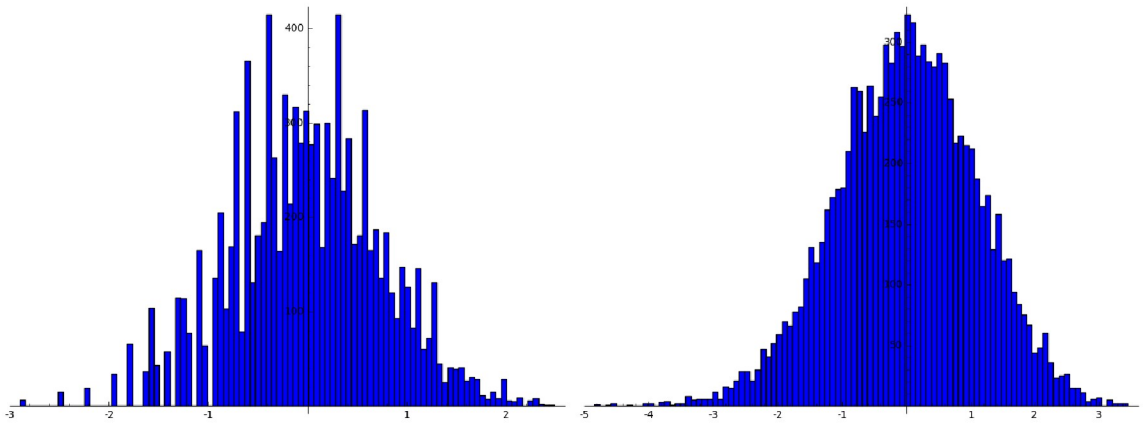


Figure 2.1: Naturalized Class Number for $D_0 = 10^5$ (left) and 10^{15} (right)

A representative sample of figures is included in this chapter. For a more complete set of figures, see Appendix A.

In the section on factor bases, we will discuss how class groups can be understood as cokernels of integer matrices. Our heuristic tries to model the naturalized class group as the cokernel of a *random* integer matrix. In the chapter on random matrices, we also discuss how, given a choice for $n(D)$, we can choose the appropriate $X(D)$ such that matrices $A_n \in M_{n(D)\times n(D)}$ with entries taken from $N(0, X)$ are distributed with a mean that aligns with that of the class numbers. For our tests here, we numerically compute $X(D)$ for various trial choices of $n(D)$, and compare naturalized class numbers with values of $\log|\det A_n|$

2.2 Sample Data

We have normalized all our results so that data sets have mean 0.

For $D_0 = 10^5$, the distribution does not look particularly close to gaussian, but in Figure 2.1 we see that by $D_0 = 10^{15}$ we already have good convergence. To demonstrate that this really is a gaussian distribution, we compare graphs for the probablity function $P(x \leq t)$ for an appropriate range of t for naturalized class numbers and gaussians. Figure 2.2 shows these, again for the cases $D_0 = 10^5$ and $D_0 = 10^{15}$. The gaussian was a randomly

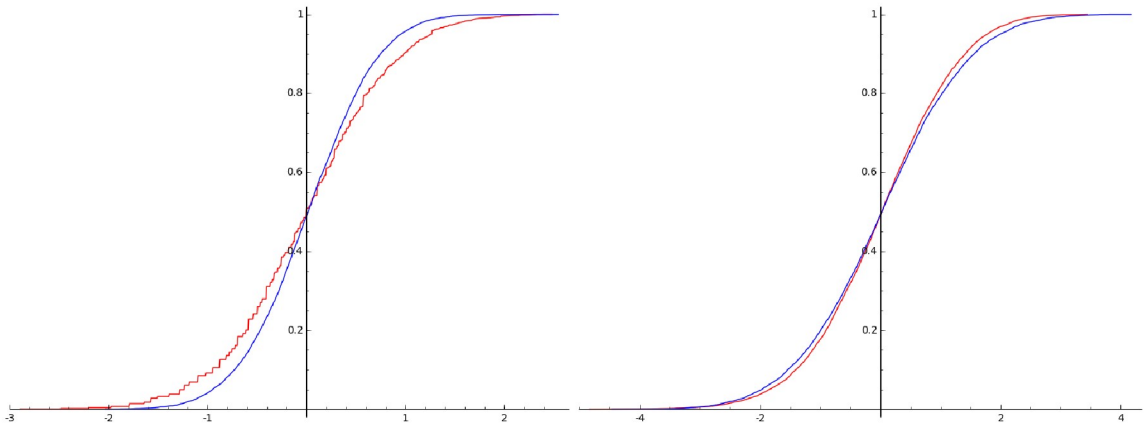


Figure 2.2: Naturalized class number for $D_0 = 10^5$ (left) and 10^{15} (right)

generated sample, also of 10000 points, sampled from a distribution having variance equal to that of the $h^\natural$ distribution. We postulated in Chapter 1 that naturalized class numbers are distributed with a variance $\log\log\log|D|^{\frac{1}{2}}$. If we look at Table 2.1, we can see that experiments are in support of this conjecture.

2.3 Matrices

Results from random matrix theory prove that as $n \to \infty$ the distribution of $\log|\det|$ for $n \times n$ matrices approaches $N(0,1)$. These results are described in the section on random matrices. Seeing that $\log h^\natural$ is already very close to gaussian in the ranges we tested there is good evidence that, at least for imaginary quadratics, $h^\natural$ can be modelled as the determinant of a random matrix of appropriate size.

So what does the distribution of the logarithm of random matrix determinants look like? Again, we sampled 10000 matrices $A_n \in M_{n\times n}$ for different n, and computed $\log|\det A_n|$. Our heuristic model suggests $n(D) \sim \log\log|D|^{\frac{1}{2}}$, which for our ranges of $|D|$ is around 2 or 3. Experimental data also supported this as the most appropriate choice for n. In Figure 2.3 we plot a similar probability curve $P(x \leq t)$ as before for $\log|\det A_n|$. The left plot compares $\log h^\natural(D)$ for $D \in [-10^24, 0]$ against $\log|\det A_n|$ for $n = 3$. On the right we include additionally a gaussian with variance equivalent to that of the $\log h^\natural$ distribution.

Table 2.1: Variance for $\log h^\natural$ vs. $\log\log\log|D|^{\frac{1}{2}}$

$\lvert D_0\rvert$	Variance for $\log h^\natural$	$\log\log\log\lvert D\rvert^{\frac{1}{2}}$
10^5	0.576	0.560
10^6	0.642	0.659
10^7	0.689	0.736
10^8	0.730	0.797
10^9	0.782	0.849
10^{10}	0.828	0.893
10^{11}	0.858	0.931
10^{12}	0.893	0.965
10^{13}	0.957	0.995
10^{14}	0.979	1.022
10^{15}	1.011	1.047
10^{16}	1.019	1.069
10^{17}	1.069	1.089
10^{18}	1.080	1.109
10^{19}	1.124	1.127
10^{20}	1.148	1.143
10^{21}	1.146	1.159
10^{22}	1.168	1.173
10^{23}	1.209	1.186
10^{24}	1.219	1.200

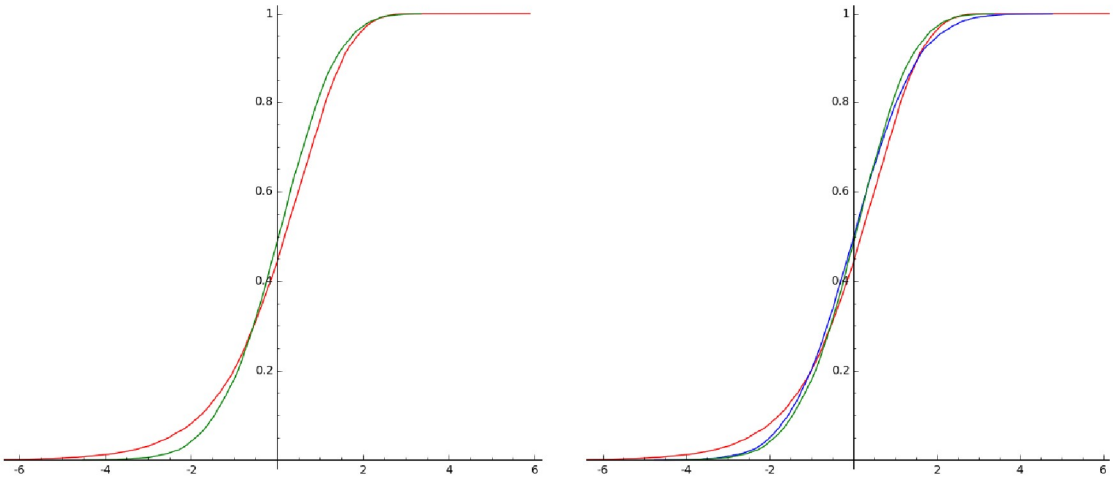


Figure 2.3: Comparing $\log h^\natural$ (green) with $\log\det|A_n|$ (red) for $D_0 = 10^{24}$. The figure on the right includes a gaussian (blue) for comparison. In this case where $n(D) = 3$, $X(D)$ was approximately 2×10^5.

Chapter 3

Predictions and Corrections from Genus Theory

We now present some theoretical calculations involving class numbers and regulators. The implications of Genus Theory, the Erdős-Kac Theorem and the Analytic Class Number formula are discussed to arrive at an expression that motivates our conjectures in Chapter 1.

3.1 Genus Theory, Erdős-Kac, and the Analytic Class Number Formula

Earlier it was mentioned that Genus Theory gives us a precise formulation of the 2-torsion subgroup of the class group of a number field K, denoted as $\mathrm{Cl}(K)[2]$. Specifically it tells us that for $K = \mathbb{Q}(\sqrt{D})$, we have $\mathrm{Cl}(K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{\omega(D)-1}$.

Clearly, then, we cannot expect our class groups to behave *entirely* like randomly matrices. A subsequent idea is to consider $\mathrm{Cl}(K)/\mathrm{Cl}(K)[2] = \mathrm{Cl}^{\natural}(K)$, for which we have no equivalently precise descriptions, and see how 'random' the distribution of this part looks.

Thus

$$h(D) = h^\natural(D)2^{\omega(D)-1}.$$

3.2 An Expression for $h^\natural R$

The **Analytic Class Number Formula** gives us an analytic expression for the class number times regulator of a quadratic extension in terms of a *Dirichlet L-Function*.

Let

$$\left(\frac{D}{p}\right) = \begin{cases} 1, & \text{if } D \text{ is a square} \pmod p \\ 0, & \text{if } p|D \\ -1, & \text{if } D \text{ is not a square} \pmod p \end{cases}$$

We define $\chi_D = \left(\frac{D}{\cdot}\right) : \mathbb{Z} \to \{-1, 0, 1\}$ by $n \mapsto \left(\frac{D}{n}\right) = \prod_{p^e|n} \left(\frac{D}{p}\right)^e$. Then, we have the following result:

Theorem 3.2.1 (Analytic Class Number Formula) *Let $h = h(D)$ be the class number and $R = R(D)$ the regulator of a quadratic field $\mathbb{Q}[\sqrt{D}]$. Then,*

$$L(1, \chi_D) = \sum_{n=1}^{\infty} \frac{\chi_D(n)}{n} = \frac{\eta h R}{\sqrt{|D|}}$$

where χ_D is as above and $\eta = 1$ if $D < 0$ and $\eta = \pi$ if $D > 0$.

Due to a theorem by Littlewood [6], we know that under the Generalized Riemann Hypothesis this infinite sum can be altered into a finite one

$$\text{GRH} \implies L(1, \chi_D) = \sum_{p \le \log \sqrt{|D|}} \frac{\chi_D(p)}{p} + O(1) \text{ for } p \text{ prime.}$$

In order to incorporate Genus Theory and get a prediction for $h^\natural(D)$, we must find a way to account for the expected number of prime divisors of the discriminant. The Erdős-Kac theorem [7] gives us an asymptotic result for this $\omega(D)$:

Theorem 3.2.2 (from Erdős-Kac) *Let $\omega(D)$ be the number of prime divisors of D. Then, for any fixed $a < b$,*

$$\lim_{x\to\infty}\left(\frac{1}{x}\cdot\#\left\{n\le x : a\le\frac{\omega(n)-\log\log n}{\sqrt{\log\log n}}\le b\right\}\right)=\Phi(a,b)$$

where $\Phi(a,b)=\frac{1}{\sqrt{2\pi}}\int_a^b e^{-t^2/2}dt$ is the standard Gaussian distribution. This in turn implies that

$$\omega(D)\in[(1-\mu)\log\log|D|,(1+\mu)\log\log|D|]$$

for any fixed $\mu>0$ with probability $1-o(1)$, as $|D|\to\infty$.

By estimating $\sum_{p\le x}\frac{\chi_D(p)}{p}$ as $\log\log(x)+\gamma+o(1)$ in the Analytic Class Number formula (where γ is the Euler gamma function) we get:

$$\log\eta+\log(hR)-\log|D|^{1/2}=\log\log\log|D|^{1/2}+\log(e^{\gamma})+o(1),\text{ or}$$
$$\log(hR)=\log|D|^{1/2}+\log\log\log|D|^{1/2}+\log(e^{\gamma}/\eta)+o(1)$$

Since $h = h_2h^\natural$ where $h_2=\#\operatorname{Cl}(K)[2]$, and from Erdős-Kac we have $\log h\asymp\log h^\natural+\log 2(\log\log|D|-1)=\log h^\natural+\log 2\log\log|D|-\log 2$, we get:

$$\log(hR)=\log(h_2h^\natural R)\asymp\log(h^\natural R)+\log 2\log\log|D|-\log 2$$

Putting this all together, we finally get:

$$\log(h^\natural R)\asymp\log|D|^{1/2}-\log 2\log\log|D|+\log\log\log|D|^{1/2}+\log(2\frac{e^{\gamma}}{\eta})+o(1)\quad(3.1)$$

which gives a prediction for the logarithm of the naturalized class number times regulator.

From the Brauer-Siegel theorem, we know that $\log h(D)R(D)\to\log|D|^{\frac{1}{2}}$ as $D\to\infty$, this matches with the first term of the formula. Estimating the size of $\omega(D)$ from Erdős-Kac gives us the Genus Theory correction that is the second term, so we expect that $\log(h^\natural R)$ has mean $\log|D|^{1/2}-\log 2\log\log|D|$. This suggests that the third term, $\log\log\log|D|^{\frac{1}{2}}$, represents the variance of the distribution for $h^\natural R$ (note that experimentally we have already

seen that $h^\natural R$ looks like a normal distribution). In Chapter 5, we will relate this term to the variance term in the distribution of $\log|\det|$ of random matrices, which we know is normally distributed. This will give us the expression for $n(D)$ that we used in our conjecture in Chapter 1.

Chapter 4

Class Group Over a Factor Base

From a theorem due to Minkowski, we can deduce a bound on the norm of the ideals we need to check in order to recover the class group. The theorem in the quadratic case states that every class in the class group contains a representative ideal of norm explicitly bounded in terms of $|D|$, on the order of $\sqrt{D}$. The class group, then, is generated by prime ideals under the Minkowski bound. From here, we also get a quick proof of the finiteness of the class group– since there are only finitely many ideals below the Minkowski bound, there can only be finitely many classes in the class group.

Under the Generalized Riemann Hypothesis, the bound on ideals to be checked can be brought down to $6(\log |D|)^2$. The lowering from a $\sqrt{|D|}$ dependence to a $\log |D|$ dependence considerably simplifies the computation of the class group for number fields of large discriminant.

4.1 Generators and Relations

Using this bound we can represent the class group of a number field K in matrix form. For an extension $K/\mathbb{Q}$ take primes $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \ldots, \mathfrak{p}_n$ below the Minkowski bound. We know with certainty that these primes generate the class group (of course in reality a smaller subset may be sufficient). Now, take elements $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_m$ from the ring of integers

$\mathbb{Z}_K$, that factor amongst these primes. Since any ideal (α_i) is principal, it corresponds to the identity in the class group, and so each factorization represents a relation amongst group elements in the class group. We simply wish to find enough relations to capture all necessary information about the class group. It may not be initially clear how many relations we need to consider, but since they are drawn from some finite set (there are finitely many ideals and finitely many powers of them that still lie below the Minkowski bound) there is an upper limit to how many independent relations we need to consider.

For $0 \leq i \leq m$, say $(\alpha_i) = \mathfrak{p}_1^{e_{i1}}\mathfrak{p}_2^{e_{i2}}\mathfrak{p}_3^{e_{i3}} \dots \mathfrak{p}_n^{e_{in}}$. Then we construct the following matrix:

$$\begin{pmatrix} e_{11} & e_{12} & \dots & e_{1n} \\ e_{21} & e_{22} & \dots & e_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ e_{m1} & e_{m2} & \dots & e_{mn} \end{pmatrix}$$

If $m < n$, we need to add more relations to the matrix, $m > n$ so far poses no concerns. Taking the Smith Normal form of this generators and relations matrix now gives us the cokernel of the matrix as a direct product of abelian groups. If we recall how the matrix was constructed, i.e. by taking powers and products of prime ideals that multiply to the identity, we immediately see that this cokernel in fact returns our class group. The determinant of the $n \times n$ matrix that is formed by removing extra rows from the matrix (in case $m > n$) is the order of the cokernel, or alternatively the class number.

By expressing the matrix in Smith normal form, we can simply read off the structure of the class group. Specifically, the group is isomorphic to $\mathbb{Z}/a_1\mathbb{Z} \oplus \mathbb{Z}/a_2\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/a_n\mathbb{Z}$ where the a_i's are the diagonal entries in the Smith normal form of the generators and relations matrix.

Thus we have a representation of the class group, in terms of generators and relations, as the cokernel of a matrix, and of the class number as the determinant. The aim of this thesis is to consider whether these matrices can be considered 'random' in some sense, and what the distribution of class numbers converges to (if anything) as the discriminants tend

to infinity.

4.2 Example

Let us consider an easy example of constructing a generators and relations matrix. For the field $\mathbb{Q}[\sqrt{-5}]$, the associated ring of integers is $\mathbb{Z}[\sqrt{-5}]$. The Minkowski bound is around 3 in this case, so let us factor some ideals into primes with norm < 3. In reality, the bound is below 3, so we only need to consider ideals of norm 2. However, for the sake of not making this a near-trivial case, let's stick with 3 as our bound.

Some initial ideals that factor into primes below this bound are:

$$(2) = (2, 1 + \sqrt{-5})^2$$
$$(3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$$
$$(1 + \sqrt{-5}) = (2, 1 + \sqrt{-5})(3, 1 + \sqrt{-5})$$

So with $\mathfrak{p}_1 = (2, 1 + \sqrt{-5}), \mathfrak{p}_2 = (3, 1 + \sqrt{-5}), \mathfrak{p}_3 = (3, 1 - \sqrt{-5})$ and $\alpha_1 = 2, \alpha_2 = 3, \alpha_3 = 1 + \sqrt{-5}$, we create our matrix:

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

The smith normal form of this matrix is:

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

From this we see that the class group is $\mathbb{Z}/2\mathbb{Z}$, and the class number is 2, as expected.

Chapter 5

Random Matrices

This chapter introduces some results on the distribution of the determinants of random matrices. We subsequently compare the results on these determinants with our expression for naturalized class numbers and regulators in (3.1.1). The results of this comparison lead to the formulation of the model presented in Chapter 1.

5.1 The Distribution of Random Determinants

There are a number of theorems proved in recent years concerning the distribution of determinants of random matrices. One of the important outcomes of modelling class groups by random matrices is that these theorems can now be applied to make conjectures about the distribution of class numbers and class groups. We now discuss some results on random matrices that allow us to compare data on matrices and class groups directly. A close correlation of the data would make it a plausible claim that the generators and relations matrix for an arbitrary class group looks random.

What do determinants of random matrices look like? Nguyen and Vu [8] showed that for $n \times n$ matrices A_n whose entries are independent real random variables with mean zero

and variance one,

$$\frac{\log(|\det A_n^2|) - \log(n-1)!}{\sqrt{2\log n}} \to N(0,1)$$

where $N(0,1)$ is the normal distribution with mean zero and variance one. This gives, equivalently,

$$\frac{\log(|\det A_n|) - \frac{1}{2}\log(n-1)!}{\sqrt{\frac{1}{2}\log n}} \to N(0,1)$$

.

This built upon earlier results of Goodman [9] and a paper on the distribution of Bernoulli random matrices by Tao and Vu [10]

Nguyen and Vu also provide a more intuitive argument for why one should expect matrices with gaussian iid entries to have normally distributed values for the $\log$ of their determinants. This is based on an observation they credit to Goodman in [9], that in this case $\det A_n^2$ can be written as a product of χ^2 random variables. This implies that $\log\det A_n^2$ is a sum of χ^2 random variables, and so they argue we can expect some form of central limit theorem to hold.

5.2 Relating Class Groups to Random Matrices

From Nguyen and Vu's results, we expect $A_n \in M_{n\times n}$ with iid N(0,1) entries to have mean of $\log|\det A_n| = \frac{1}{2}\log(n-1)!$ and variance $\frac{1}{2}\log n$. We proposed that the variance term in (3.1.1) would be $\log\log\log|D|^{\frac{1}{2}}$, so comparing these two suggests $\log\log\log|D|^{\frac{1}{2}} \sim O(\log n(D))$. This gives us a guess for $n(D)$ as $(\log\log|D|^{\frac{1}{2}})^{O(1)}$. Experimental data in Table 2.1 indicates that the variance for naturalized class numbers looks close to $\log\log\log|D|^{\frac{1}{2}}$, so a neat guess is $n(D) \to \log\log|D|^{\frac{1}{2}}$ as $|D| \to \infty$.

For $|D|$ ranging from 10^7 to 10^{25}, this gives $n(D)$ around 2 or 3 and variance between 0.7 and 1.2. This agrees with our experimental data showing a good match for $\log h^\natural$ in the imaginary case with $\log|\det A_n|$ of matrices of this size, as well as the appropriate ranges

for variance.

Since we expect our $n(D) \times n(D)$ matrix to have $\log\det \sim \frac{1}{2}\log(n(D)-1)!$, we must scale our entries to have variance greater than 1. Scaling the variance for the entries by a factor of σ^2 is comparable to scaling the values by a factor of σ, thus the overall determinant changes by a multiplicative factor of σ^n. This means that the $\log$ of the determinant changes by an additive factor of $n \log X$. Therefore, we want X such that:

$$n \log X + \frac{1}{2}\log(n-1)! = |D|^{\frac{1}{2}} - \log 2 \log\log|D|).$$

This essentially is saying that we want our mean for $\log|\det|$ to align with the mean for $h^\natural(D)R(D)$.

Let $H = \log|D|^{\frac{1}{2}} - \log 2 \log\log|D|$. Then we have:

$$n \log X = H - \tfrac{1}{2}\log(n-1)!$$

We use Stirling's approximation for $\log n!$ and get

$$\log X = \tfrac{H}{n} - \tfrac{(n-1)\log(n-1)+(n-1)-O(\log n)}{2n}$$

Since we are interested in the limit $n \to \infty$, we can eliminate terms on the right hand side that grow slower than n. Our expression simplifies to

$$\log X = \tfrac{H}{n} - \tfrac{1}{2}(\log n - 1), \text{ so substituting the expression for } H \text{ we get}$$

$$\log(X\sqrt{n}) = \log\left(\frac{D^{\frac{1}{2}}}{2^{\log\log|D|}}\right)^{\frac{1}{n}} \text{ and so we want}$$

$$\sqrt{n(D)}X(D) \to \left(\frac{D^{\frac{1}{2}}}{2^{\log\log|D|}}\right)^{\frac{1}{n}}$$

as $|D| \to \infty$, where $n(D) \to \infty$ itself, although very slowly.

The choice of $X(D)$ does not seem to affect the variance of $\log\det|A_n|$ for $n \times n$ matrices A_n, so our initial guess for $n(D) \sim \log\log\log|D|^{\frac{1}{2}}$ remains valid.

Chapter 6

The Real Quadratic Case

This chapter discuss the case of real quadratic number fields in more detail. We discuss a modification to the generators and relations matrix that helps us keep track of additional information that can be related to the regulator of the field. We propose a version of our earlier model that now applies to real quadratic fields. The real quadratic case is of particular interest because the model in this case allows us to separate the behaviours of $h^\natural(D)$ and $R(D)$, something which is not possible with the theorems like Brauer-Siegel or the Analytic Class Number formula. We also include some preliminary data to show the promise in this approach.

Computations for real quadratics appear to be much more difficult than the imaginary case. We were not able to test at a comparably high range, however the data show qualitative results that are promising for the model. Future experiments will hopefully help to smooth out any kinks and give good convergence between data and the heuristic.

6.1 Generators and Relations Matrix for Real Quadratics

We construct our generators and relations matrix along similar lines as before, but in this case we add an additional column of entries that keeps track, roughly speaking, of the archimedean "size" of each α that we factor into primes. Recall that for imaginary quadrat-

ics, we took the set of primes $\mathfrak{p}_1 \dots \mathfrak{p}_n$ below the Minkowski bound, and then factored some ideals (α_i), $\alpha \in \mathbb{Z}_K$ among these primes. The i, j^{th} entry of this matrix was then given by e^{ij}, where each α_i factored as

$$(\alpha_i) = (\mathfrak{p}_1^{e_{i1}})(\mathfrak{p}_2^{e_{i2}}) \dots (\mathfrak{p}_n^{e_{in}})$$

We now make sure to have at least $n+1$ relations, and add an extra column on the right whose entry in the i^{th} row is $\log |\alpha_i|$. This gives us an $(n+1) \times (n+1)$ matrix that looks like:

$$\left(\begin{array}{cccc|c} e_{11} & e_{12} & \cdots & e_{1n} & \log|\alpha_1| \\ e_{21} & e_{22} & \cdots & e_{2n} & \log|\alpha_2| \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ e_{(n+1)1} & e_{(n+1)2} & \cdots & e_{(n+1)n} & \log|\alpha_n| \end{array}\right)$$

Note that a unit in the field would not factor into any of the primes, and so if α_i is a unit, it would correspond to a row $\left(\begin{array}{cccc|c} 0 & 0 & \cdots & 0 & \log|\alpha_i| \end{array}\right)$

We can split this matrix into two parts. If we separate out the last column we get an $(n+1) \times n$ integer matrix– let us call this A_0. We will call the last column vector with real entries A_∞, so that our entire matrix A is $(A_0 \,|\, A_\infty)$. Since A_0 is an integer matrix, we can compute its Smith normal form. This gives us, as usual, the invariant factor decomposition of the class group. Note, however, that since this is a $(n+1) \times n$ matrix, the last row of the Smith normal form must be all zeros. This corresponds to the factorization of a unit in the field, and if we really captured all the information about our quadratic field with our chosen generators and relations it should correspond to the factorization of the *fundamental* unit ϵ. So if $S = EA_0E'$ is the Smith normal form of A_0, where E and E' are elementary matrices then the last entry of the column vector EA_∞ is $\log|\epsilon|$, or the **regulator** of the field. The determinant of the $n \times n$ matrix formed by deleting the row of zeroes from A_0 still gives us the class number h, and now the determinant of A gives us $h \log|\epsilon| = hR$.

6.2 Heuristic Model for Real Quadratics

Note that $\log(hR)$ is the quantity that appears in the Brauer-Siegel theorem for real quadratics. From this observation, and by comparison to the imaginary case, we might expect hR to look like the determinant of a random $(n+1)\times(n+1)$ matrix $A = (A_0 \,|\, A_\infty)$. However, by considering A_0 and A_∞ separately we can also disconnect our predictions about h and R. This is perhaps the most interesting feature of our heuristic model for the real quadratic case.

Model 6.2.1 *For a real quadratic field $K = \mathbb{Q}(\sqrt{D}), D \to \infty$, we model naturalized class group $\mathrm{Cl}^\natural(K)$ and regulator $\log|\epsilon|$ as follows:*
Let $n(D)$ be an integer of size $\log\log\log|D|^{\frac{1}{2}}$
$X(D)$ such that $\sqrt{n(D)}X(D) \to \left(\dfrac{D^{\frac{1}{2}}}{2^{\log\log|D|}}\right)^{\frac{1}{n}}$

Let A be an $(n+1)\times(n+1)$ matrix with structure $(A_0 \,|\, A_\infty)$, where A_0 is an $(n+1)\times n$ integer matrix with entries iid $N(0,(X(D))^2)$. Then: $\mathrm{Cl}^\natural(K)$ is modelled by the torsion subgroup of $\operatorname{coker} A_0$, and thus $h^\natural(D)$ is the determinant of the matrix formed by deleting the bottom row from the Smith normal form of A_0.

$R(D)$ is modelled by $\vec{v}\cdot A_\infty$ where $\ker A_0 = \mathbb{Z}\vec{v}$

6.3 Experimental Data

Our data is taken for 10000 randomly sampled fundamental discriminants in the range $[0, D_0]$ for $D_0 = 10^8$. While the data does not match up precisely at this order of magnitude, we see strong qualitative correlation between the heuristic prediction and actual computed values for $h^\natural(D)$ and $R(D)$. For example, we see in Figure 6.1 the heuristic model predicts appropriately sized class numbers– much smaller than in the imaginary case. In particular the predicted proportion of fields with $h^\natural(K) = 1$ is experimentally accurate. Similarly,

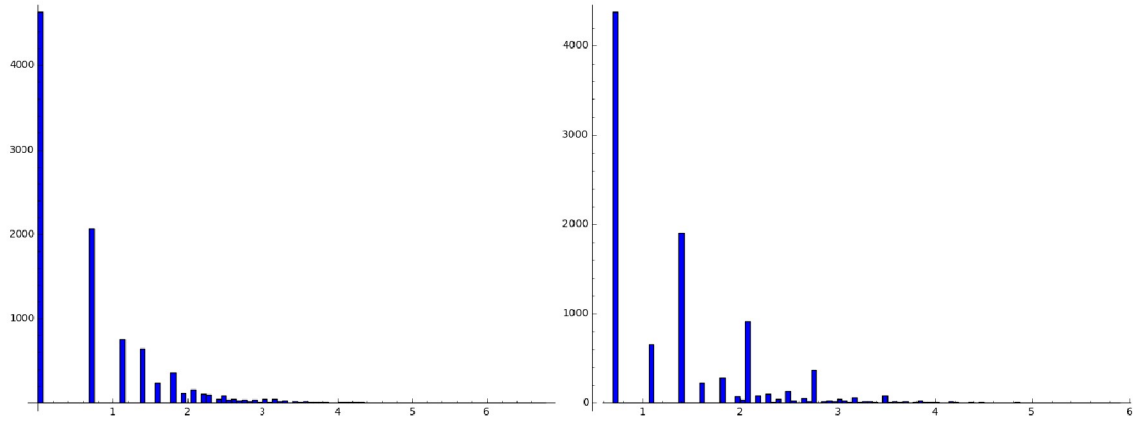


Figure 6.1: Class Number: Heuristic Prediction (left) and Sampled $\log(h^\natural(D))$ (right) for $D_0 = 10^8$

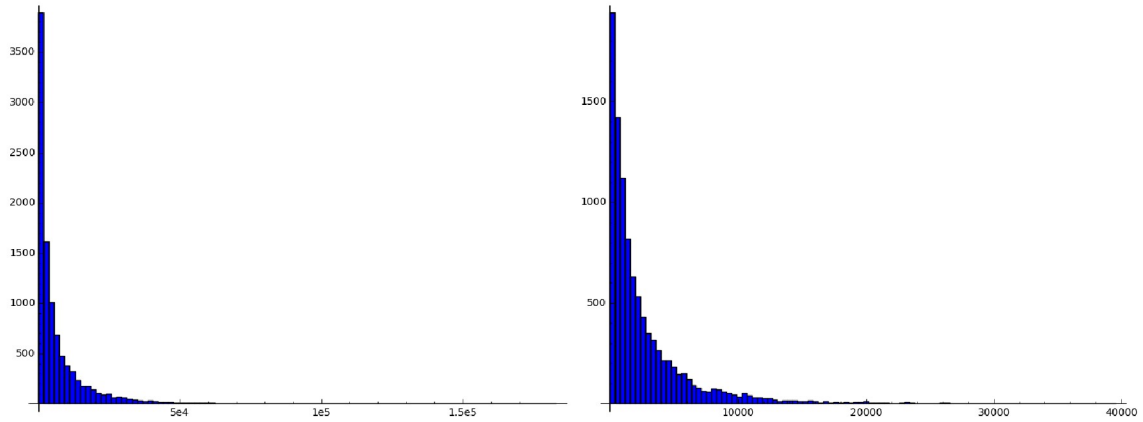


Figure 6.2: Regulator: Heuristic Prediction (left) and Sampled $R(D)$ (right) for $D_0 = 10^8$

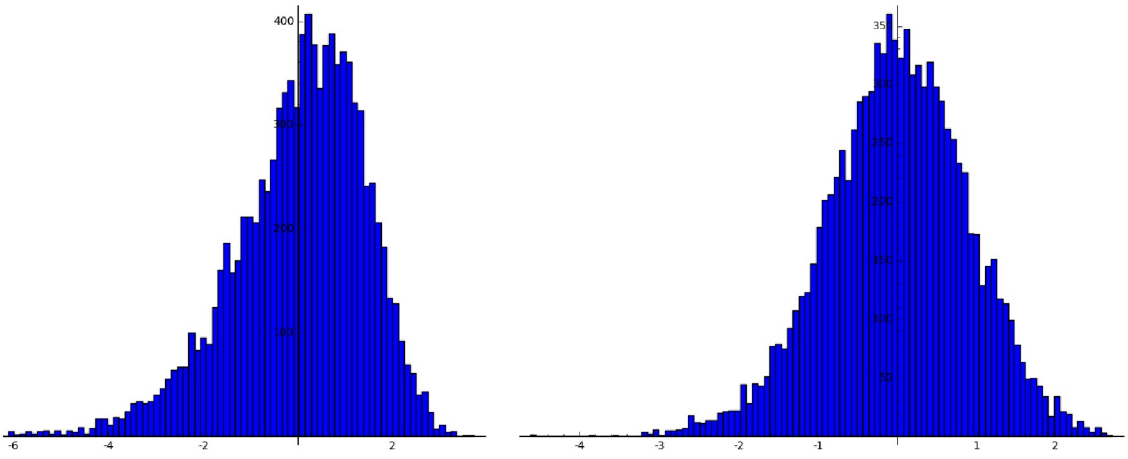


Figure 6.3: $\log(h^\natural R)$: Heuristic Prediction (left) and Sample (right) for $D_0 = 10^8$

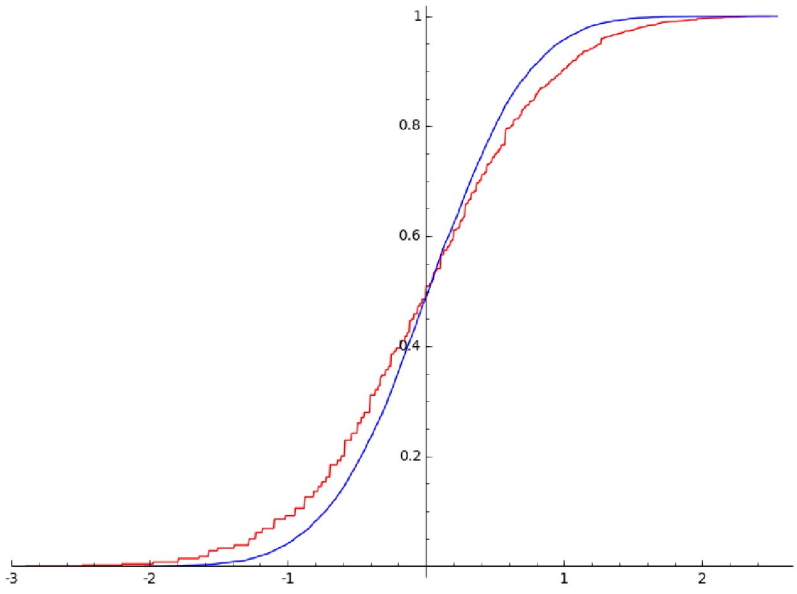
the prediction for the regulators shows appropriate trends (see Figure 6.2)

We see from Figure 6.3 that $\log|\det A|$ is still somewhat skewed compared to a gaussian. From Nguyen and Vu's theorem we expect convergence as n grows larger. Since the model is already showing behaviour that correlates qualitatively with experiments, it is expected that with computation of class groups and regulators for larger fundamental discriminant we would see a better fit numerically. With this in mind, the next step for future work is to rigorously test the heuristic for the real quadratic case with more heavy-duty experiments.

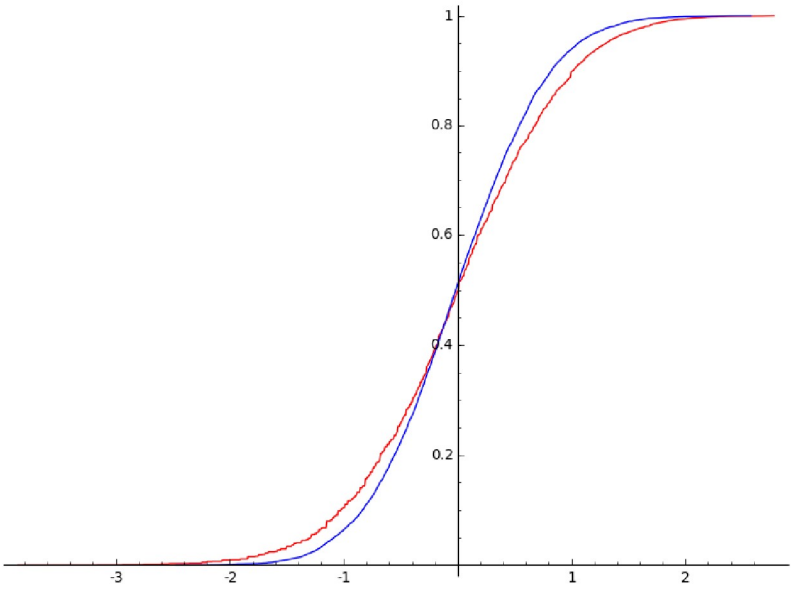
Appendix A

We include below some additional figures showing the distribution on naturalized class numbers $h^\natural(D)$ for imaginary quadratic fields, $D \in [D_0, 0]$ with $D_0 = -10^k$ for integers k between 5 and 24.

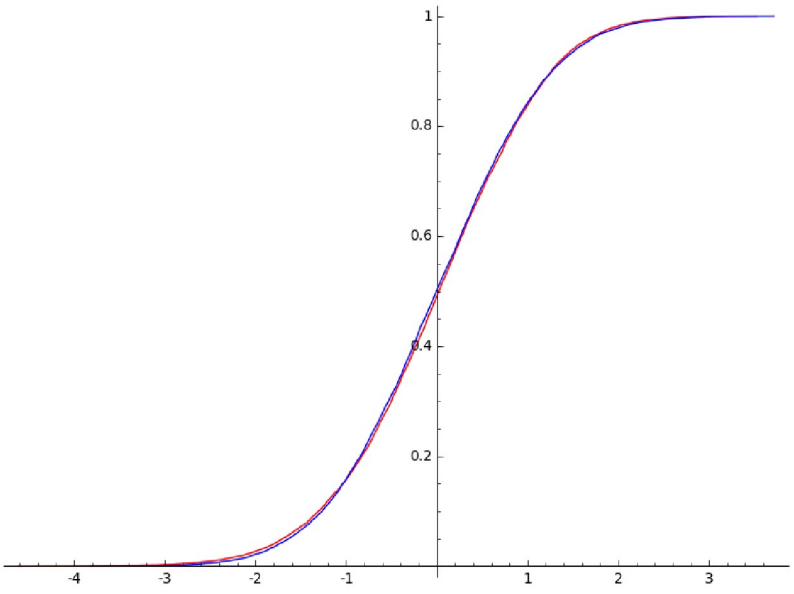
The first set of figures plots $P(x \leq t)$ for naturalized class numbers (blue) vs. a Gaussian of equivalent variance (red). The second set of figures is a direct plot of the distribution of the naturalized class numbers. For this we construct histograms with 100 bins each (10000 data points)



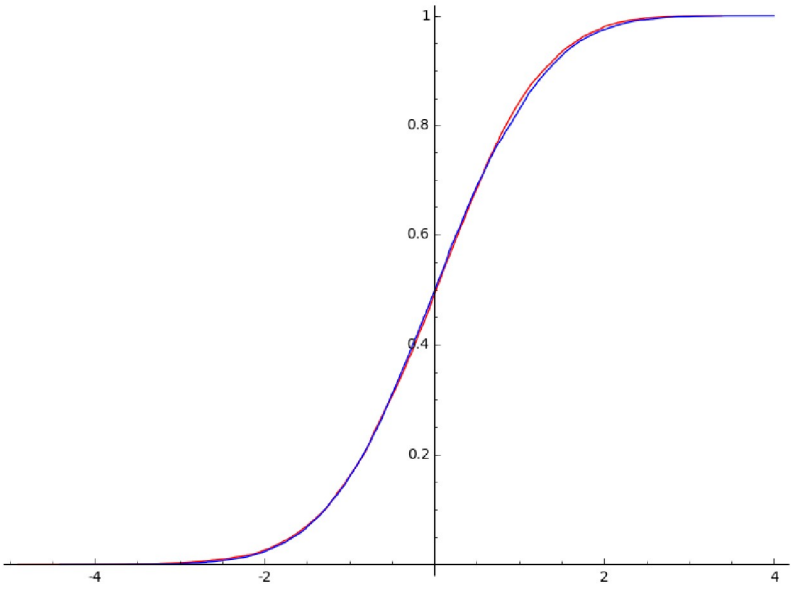
$D_0 = -10^5$



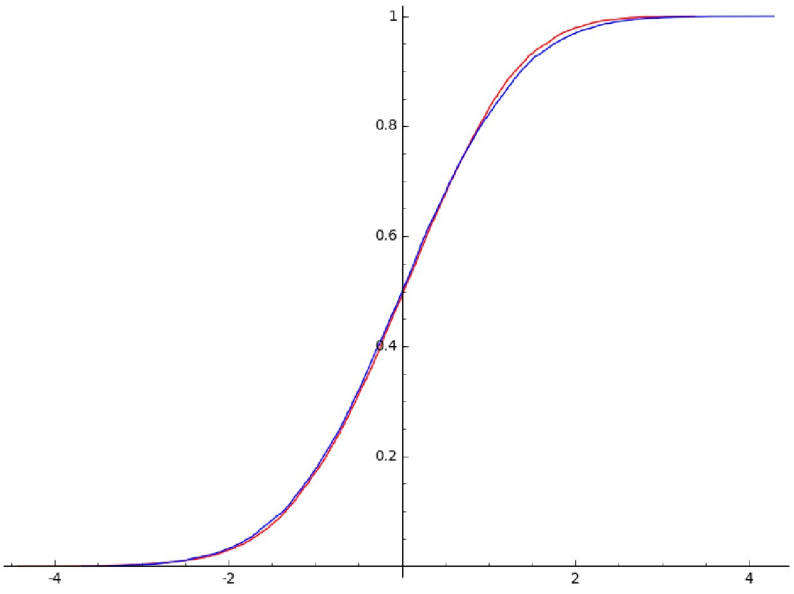
$D_0 = -10^6$



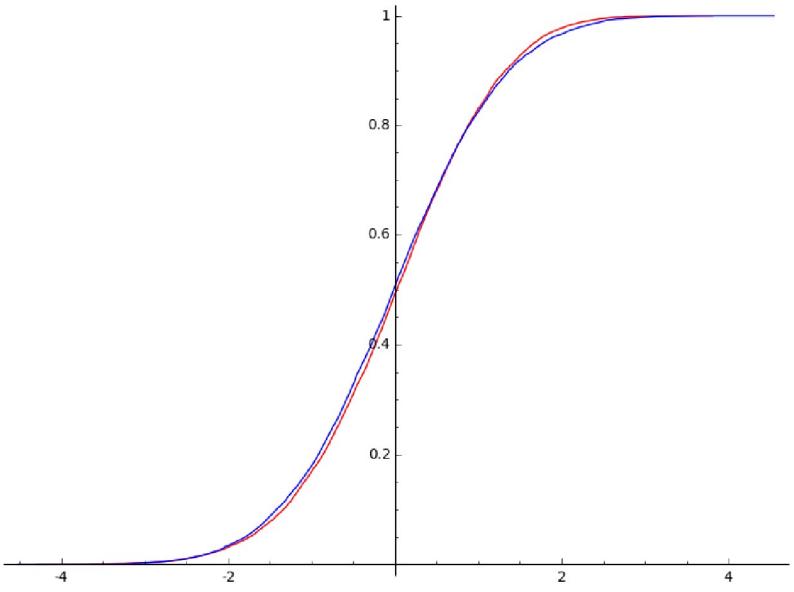
$D_0 = -10^7$



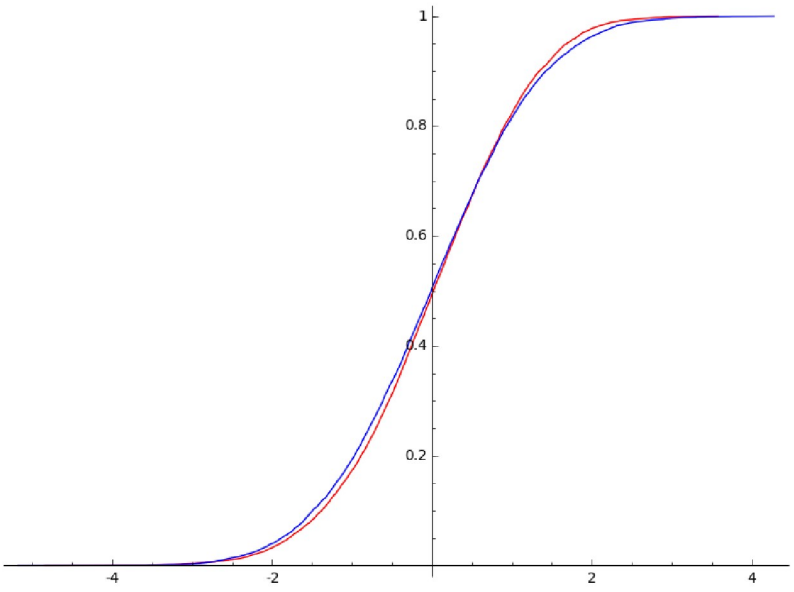
$D_0 = -10^8$



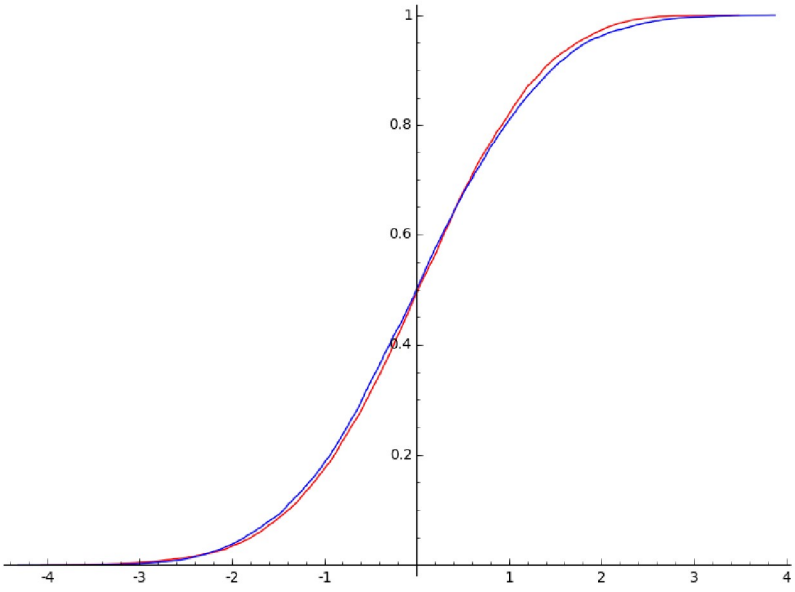
$D_0 = -10^9$



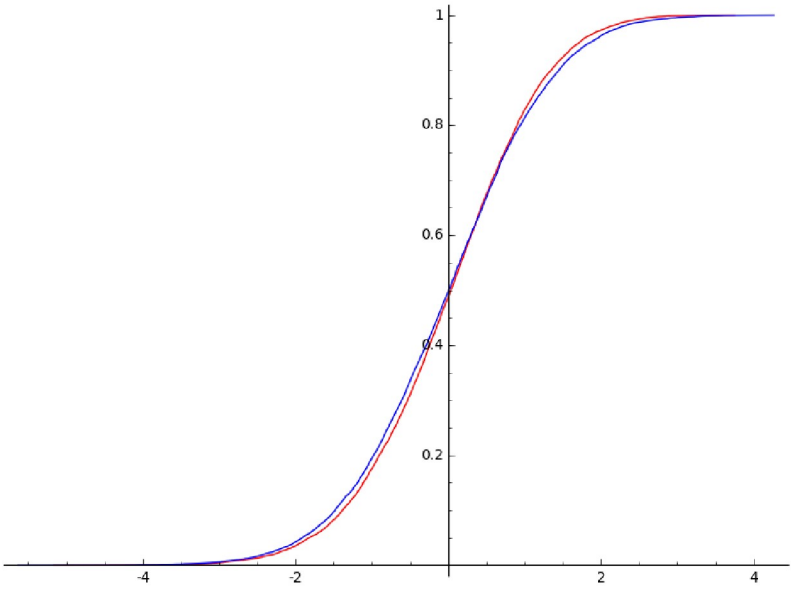
$D_0 = -10^{10}$



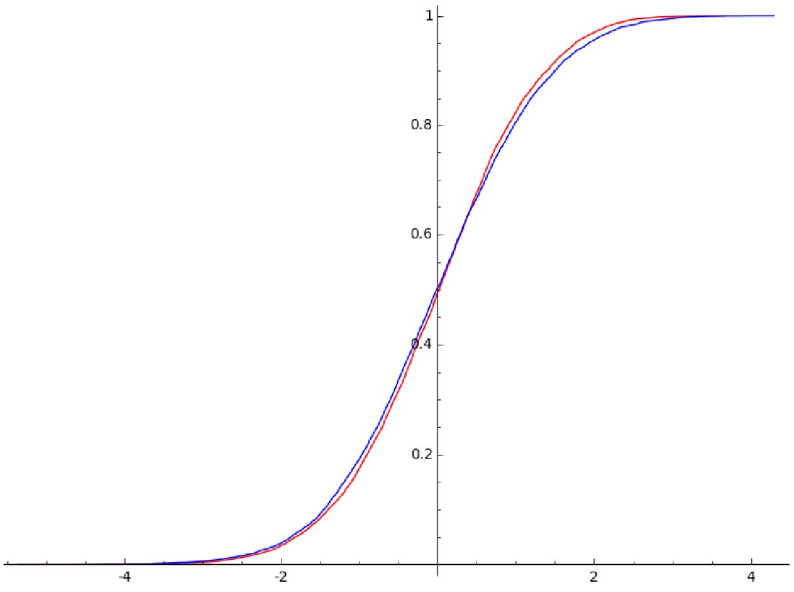
$D_0 = -10^{11}$



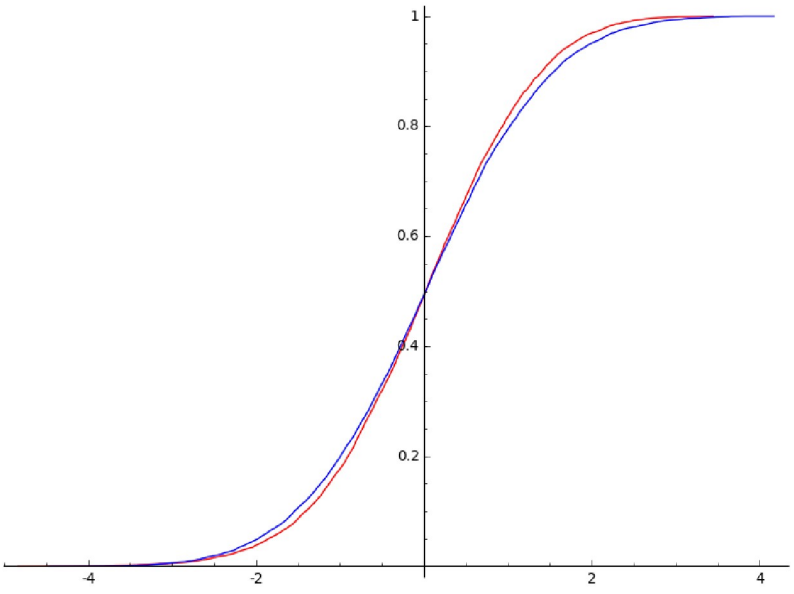
$D_0 = -10^{12}$



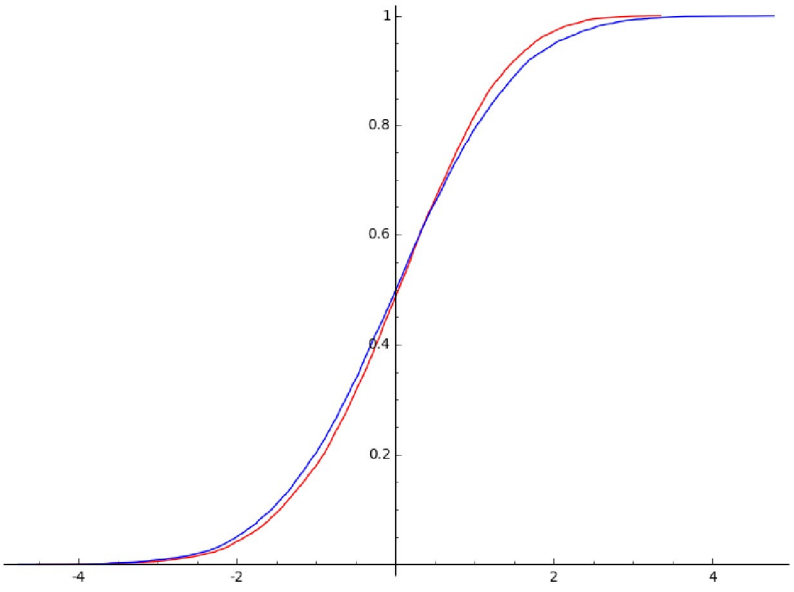
$D_0 = -10^{13}$



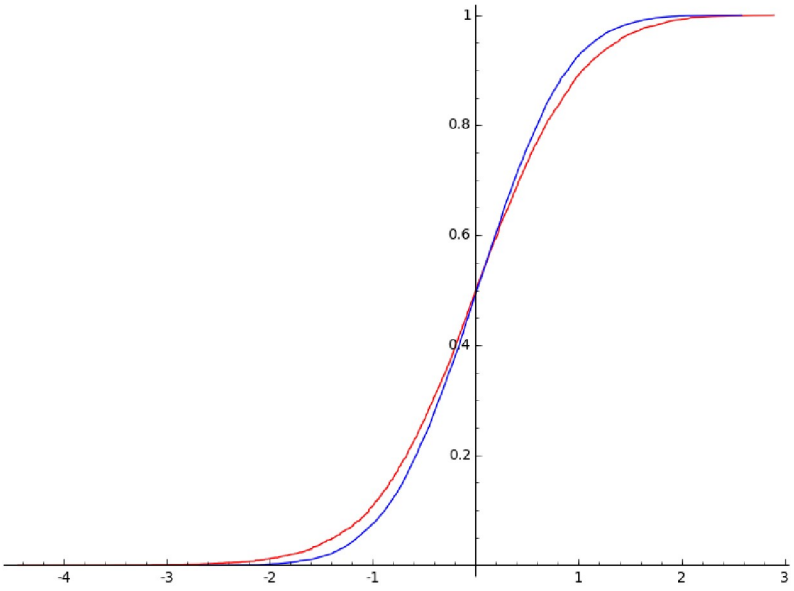
$D_0 = -10^{14}$



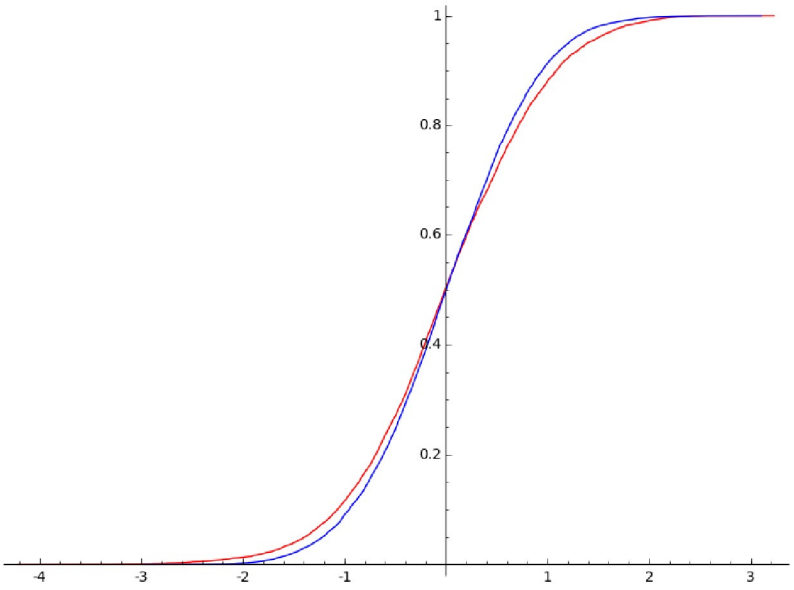
$D_0 = -10^{15}$



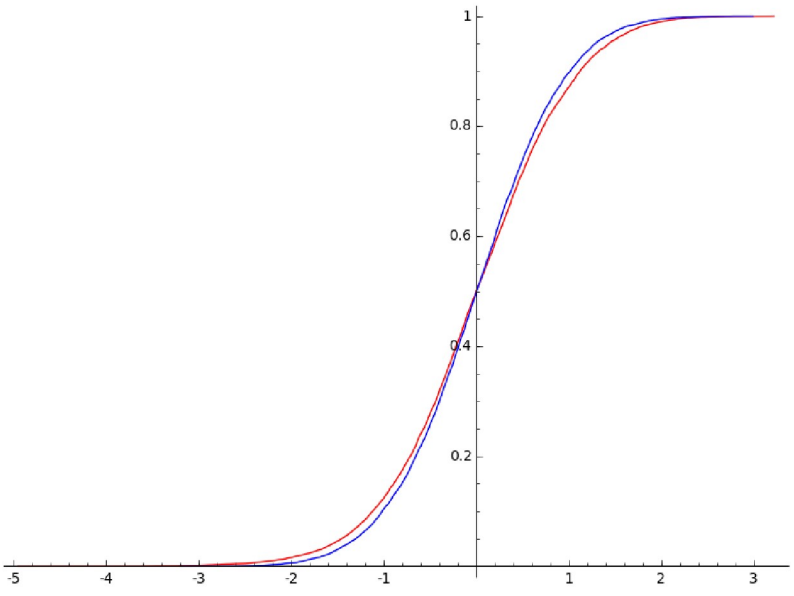
$D_0 = -10^{16}$



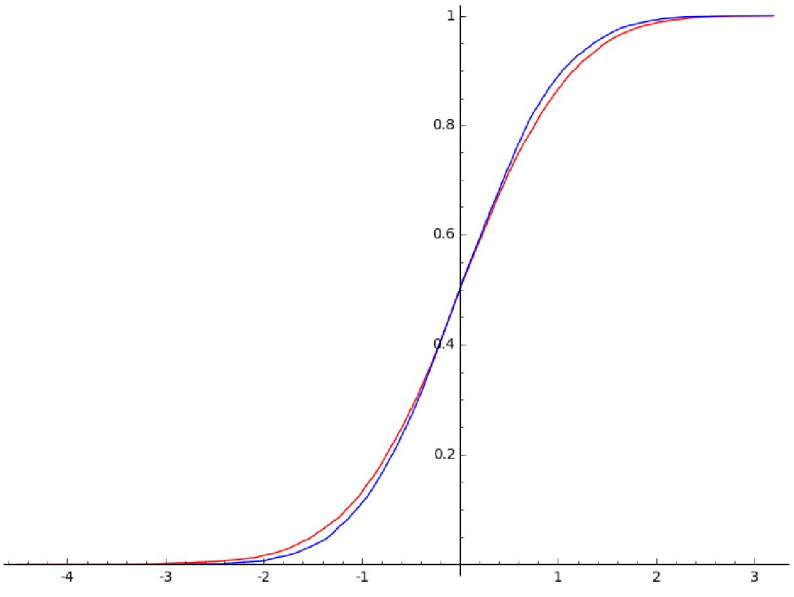
$D_0 = -10^{17}$



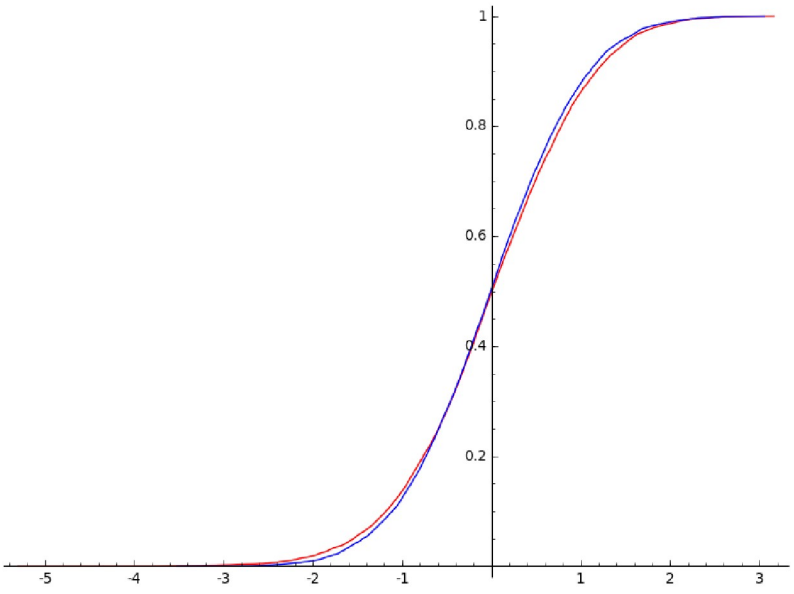
$D_0 = -10^{18}$



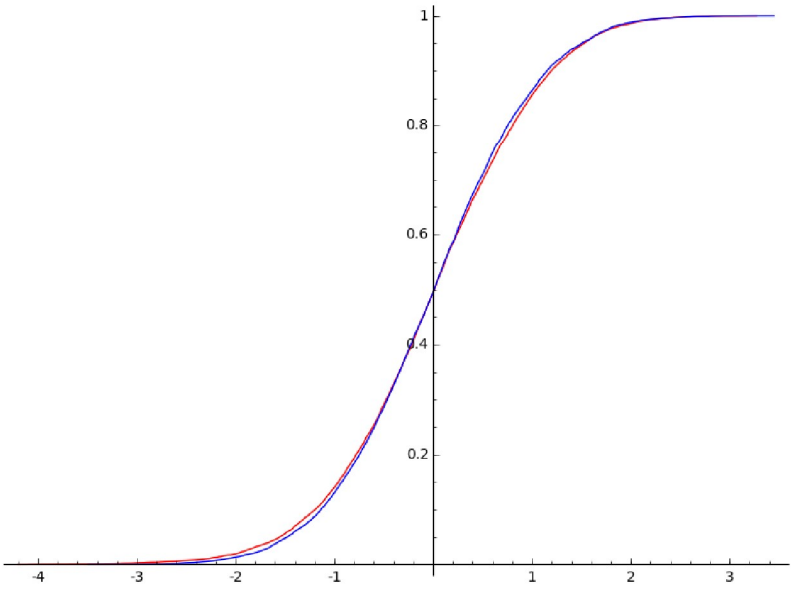
$D_0 = -10^{19}$



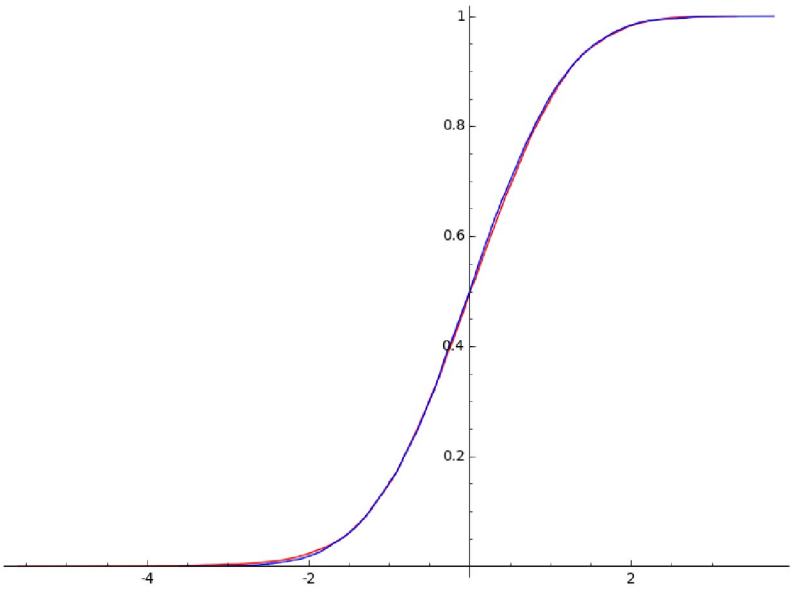
$D_0 = -10^{20}$



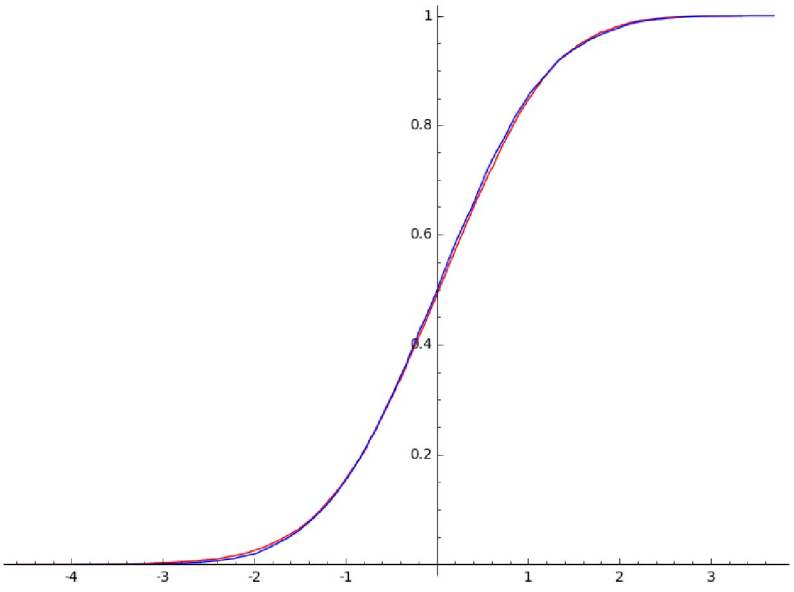
$D_0 = -10^{21}$



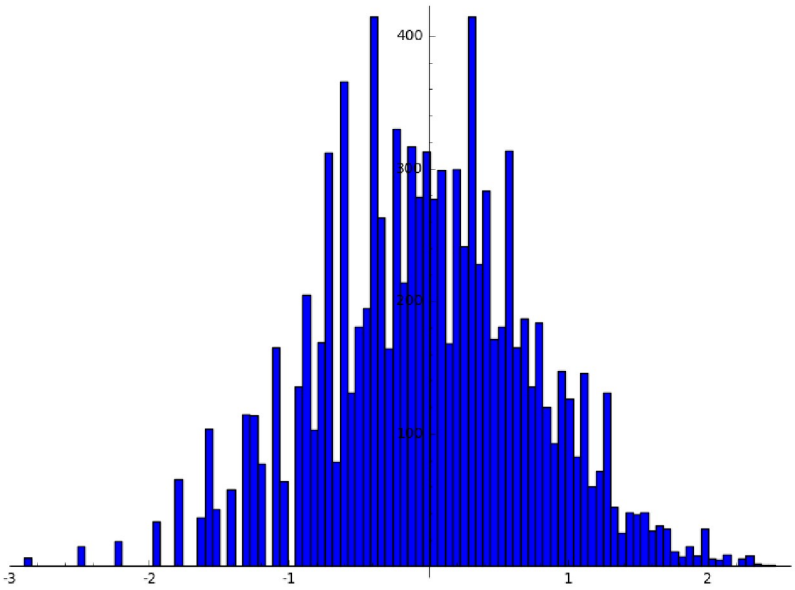
$D_0 = -10^{22}$



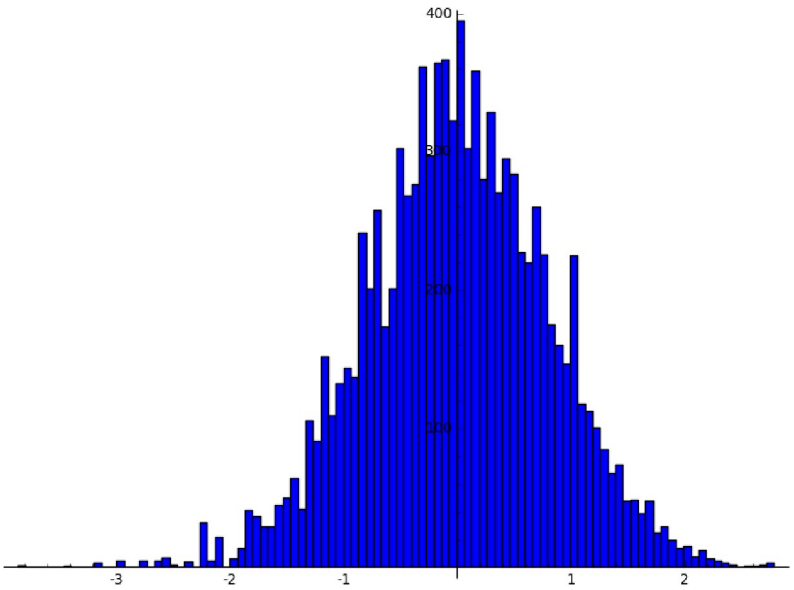
$D_0 = -10^{23}$



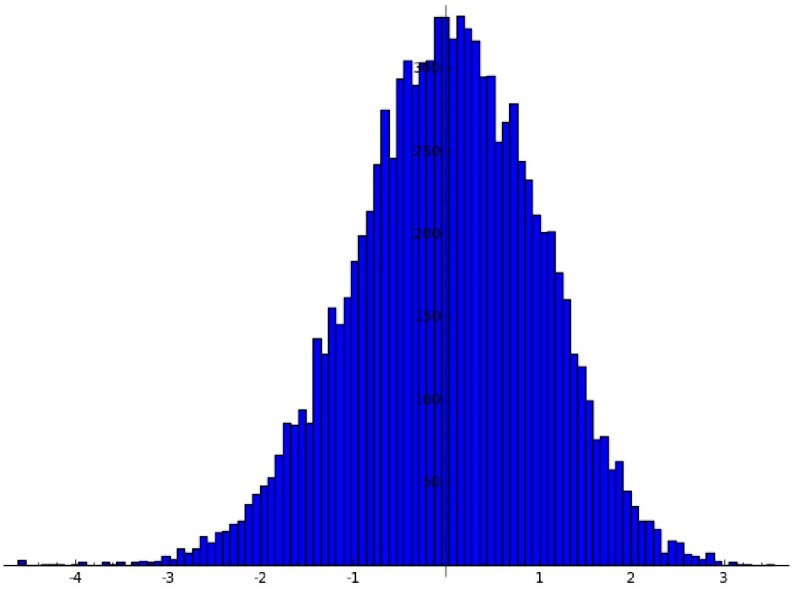
$D_0 = -10^{24}$



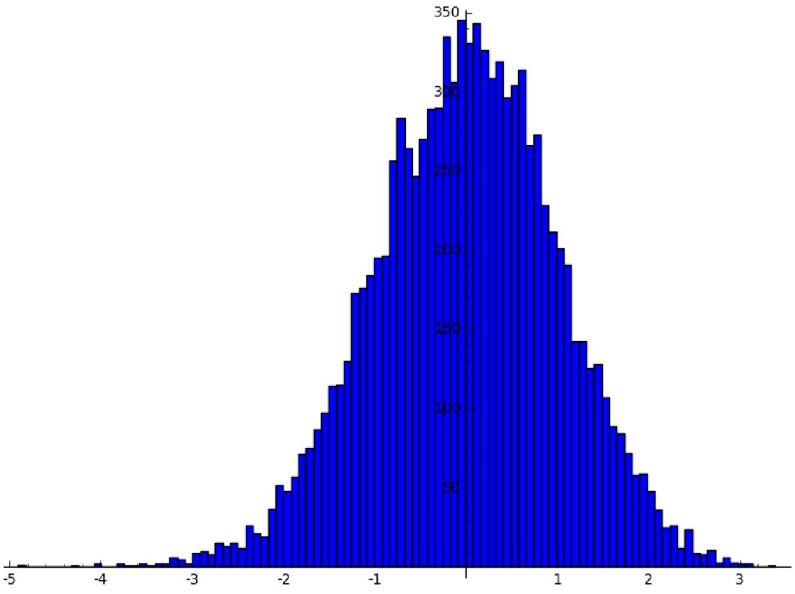
$D_0 = -10^5$



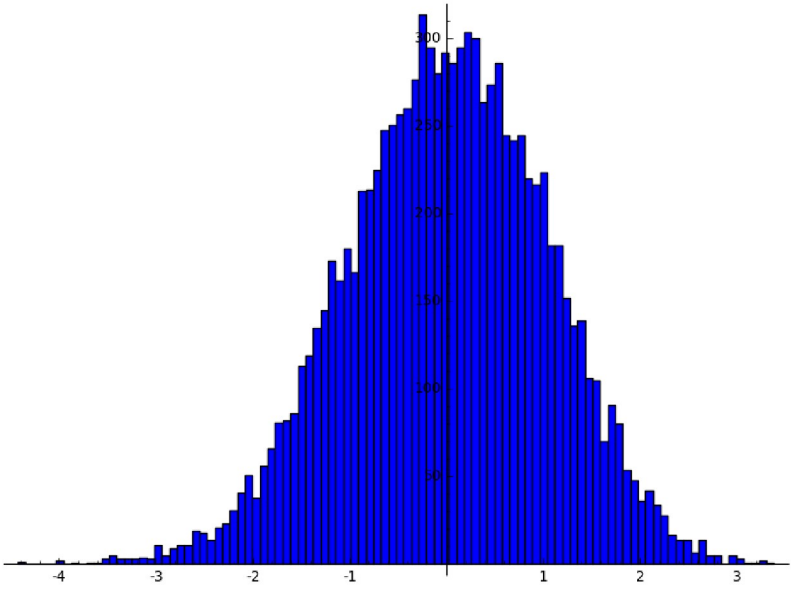
$D_0 = -10^6$



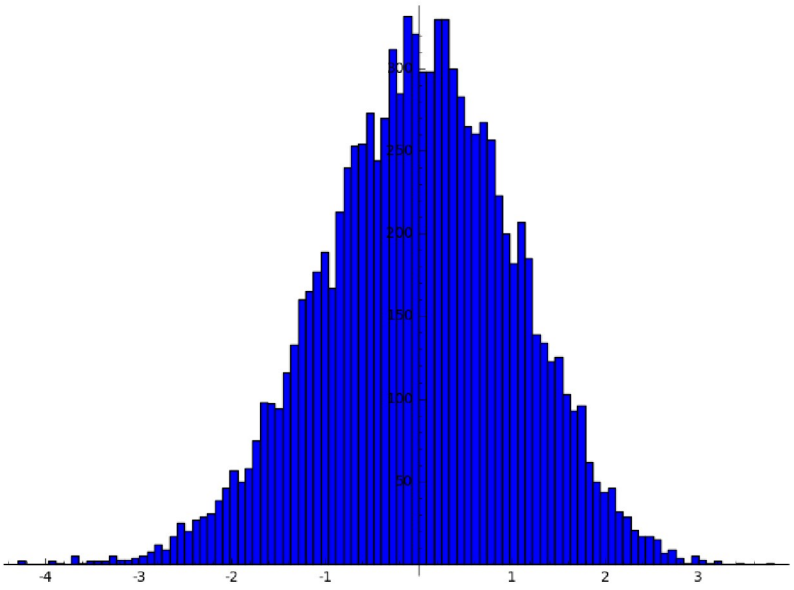
$D_0 = -10^7$



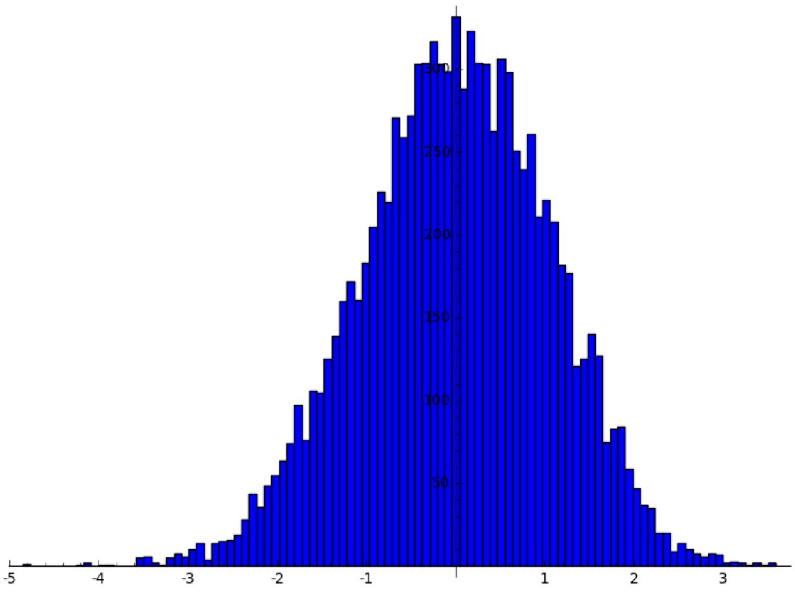
$D_0 = -10^8$



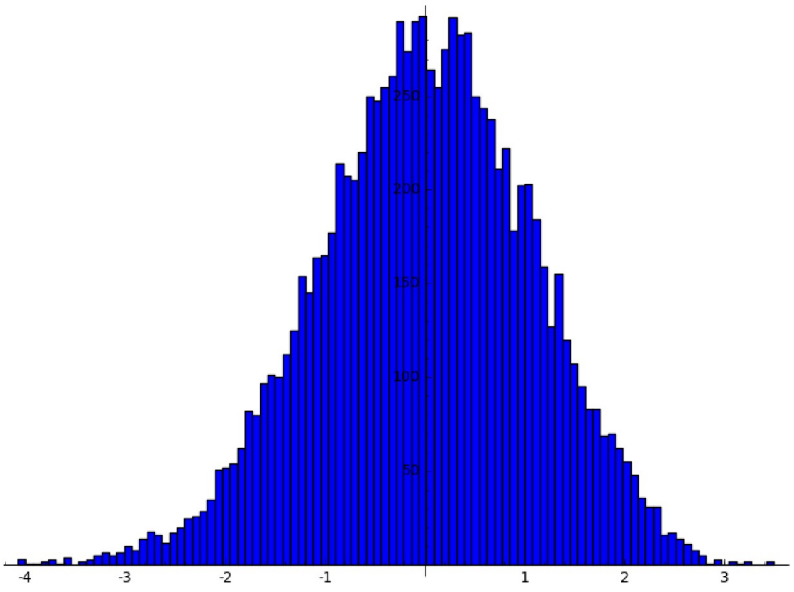
$D_0 = -10^9$



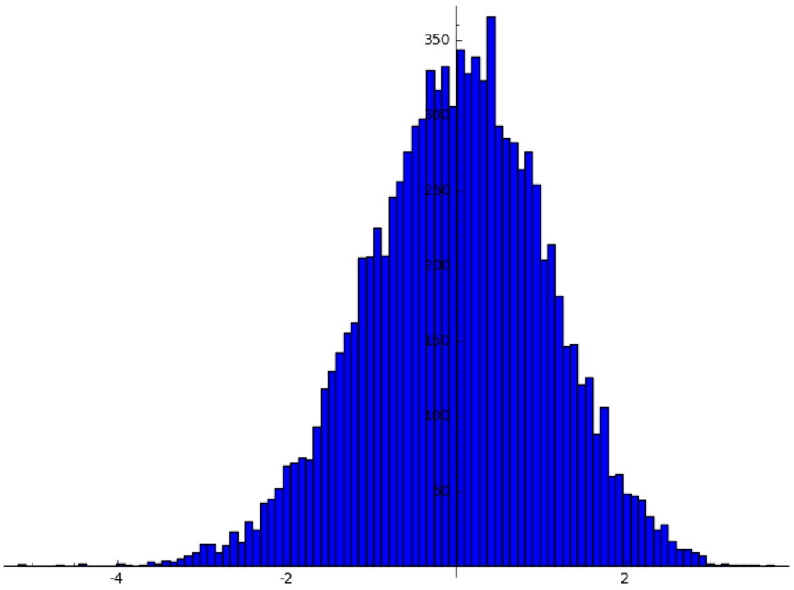
$D_0 = -10^{10}$



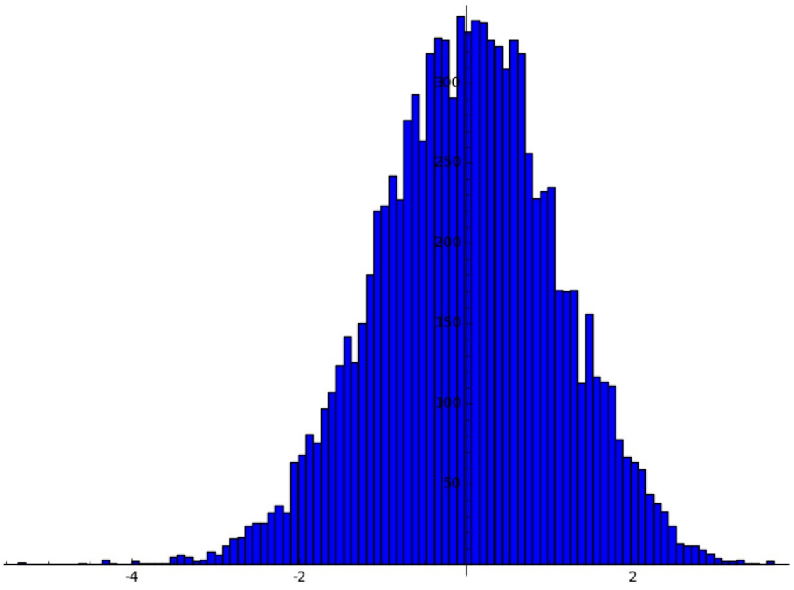
$D_0 = -10^{11}$



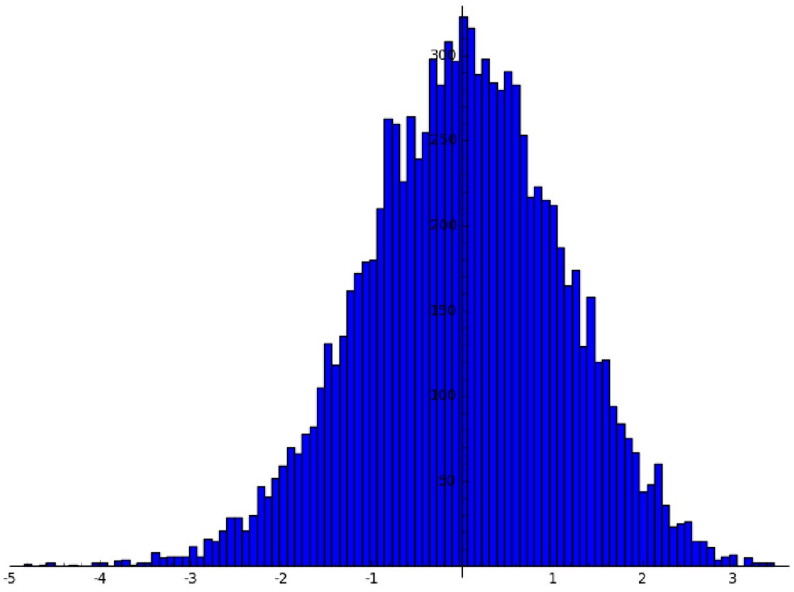
$D_0 = -10^{12}$



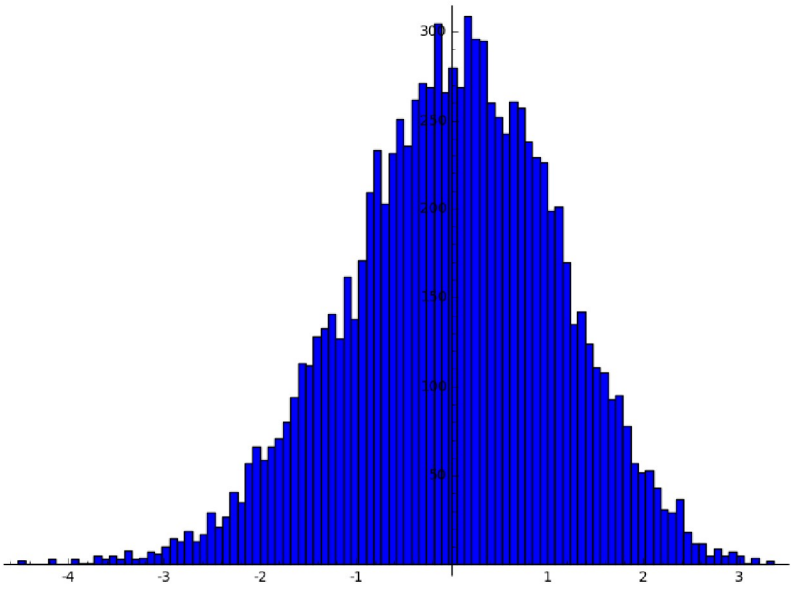
$D_0 = -10^{13}$



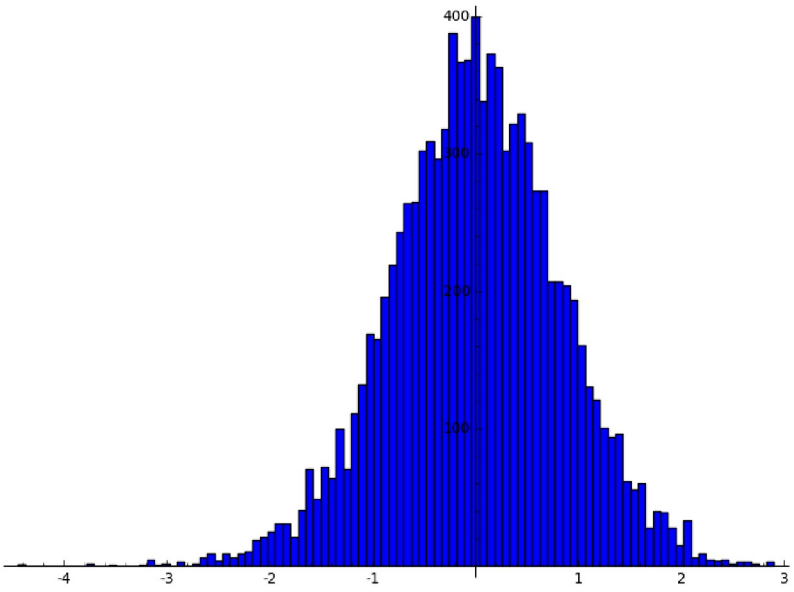
$D_0 = -10^{14}$



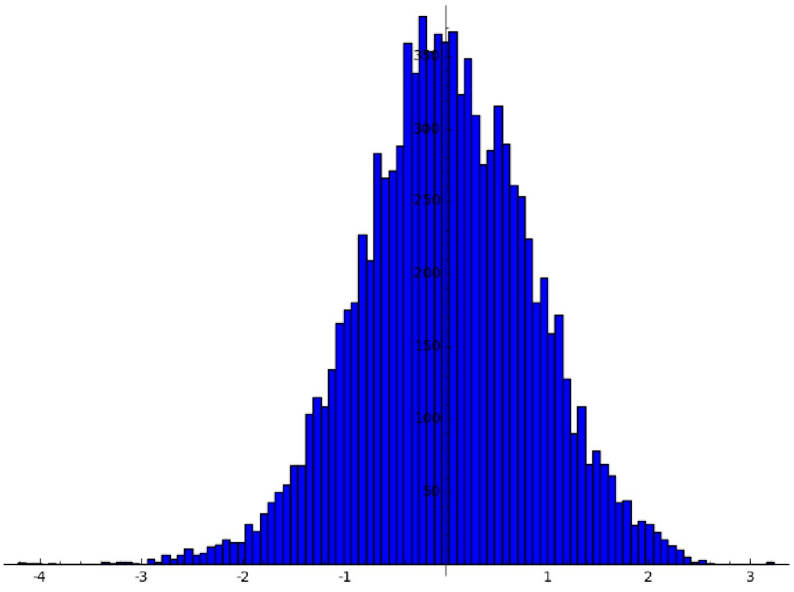
$D_0 = -10^{15}$



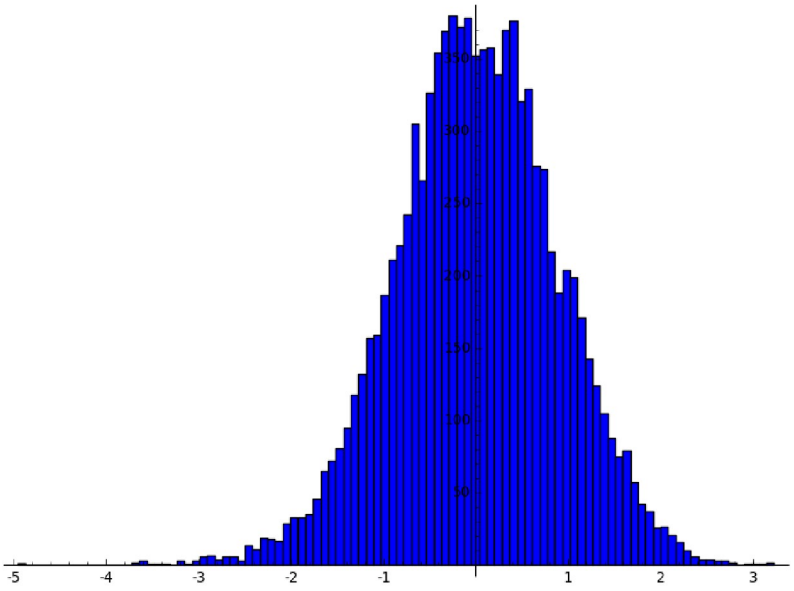
$D_0 = -10^{16}$



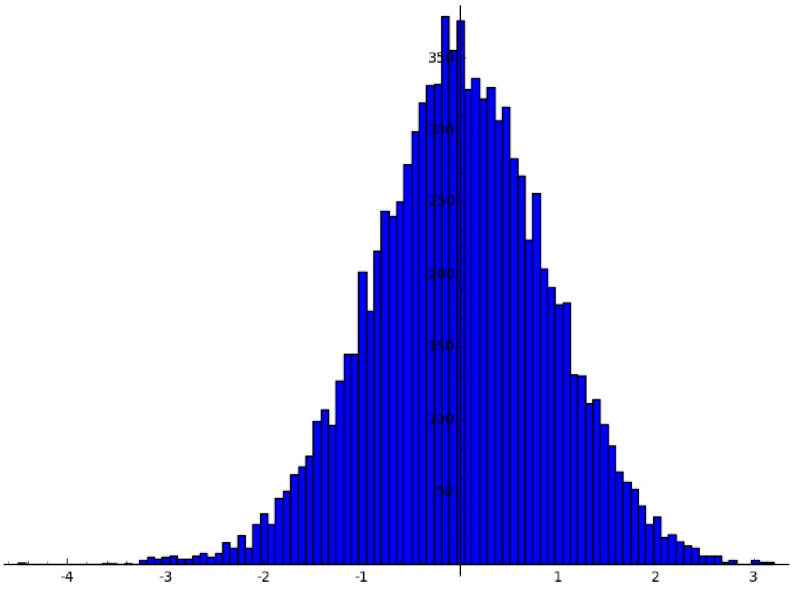
$D_0 = -10^{17}$



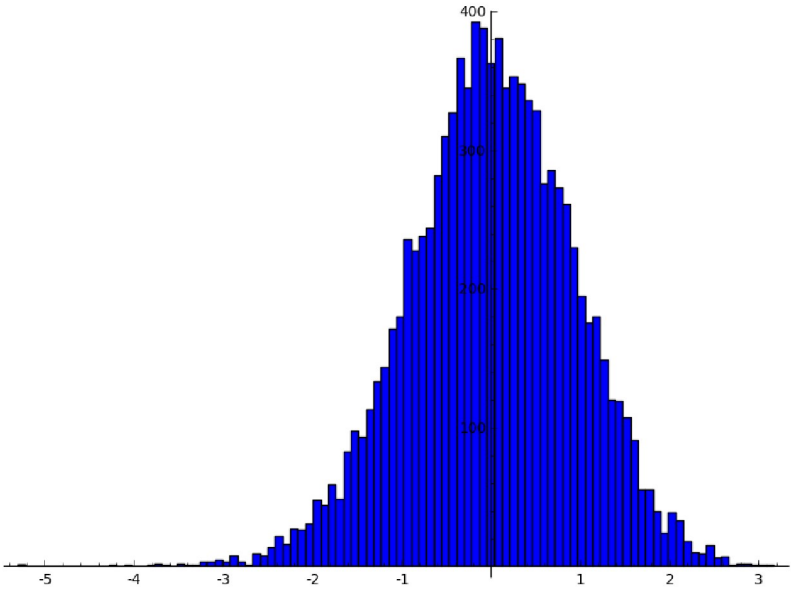
$D_0 = -10^{18}$



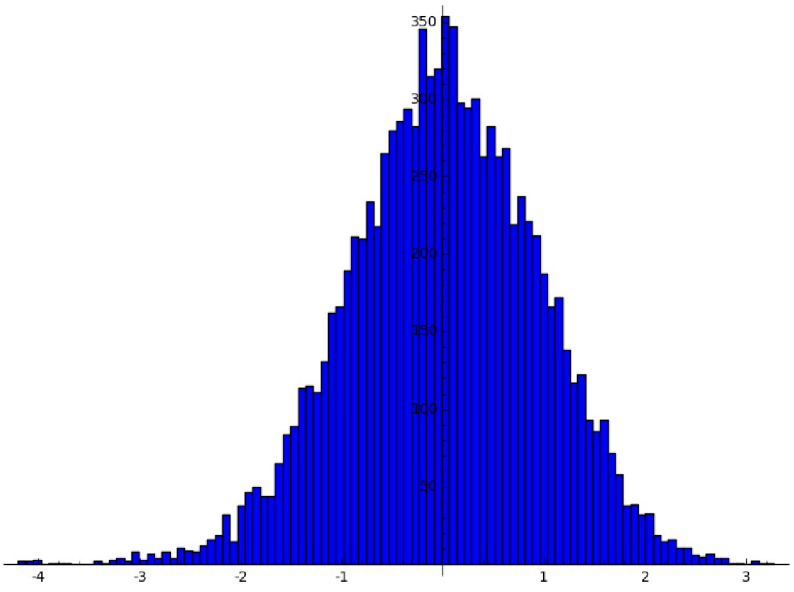
$D_0 = -10^{19}$



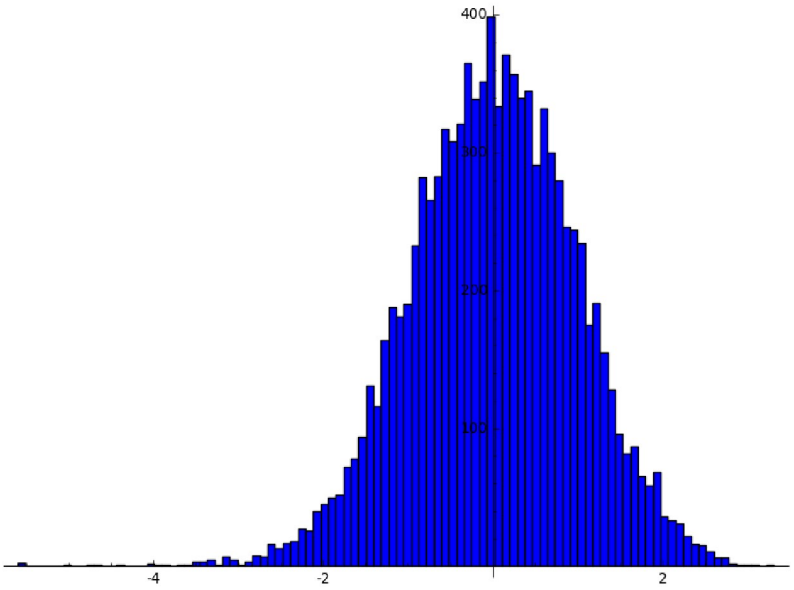
$D_0 = -10^{20}$



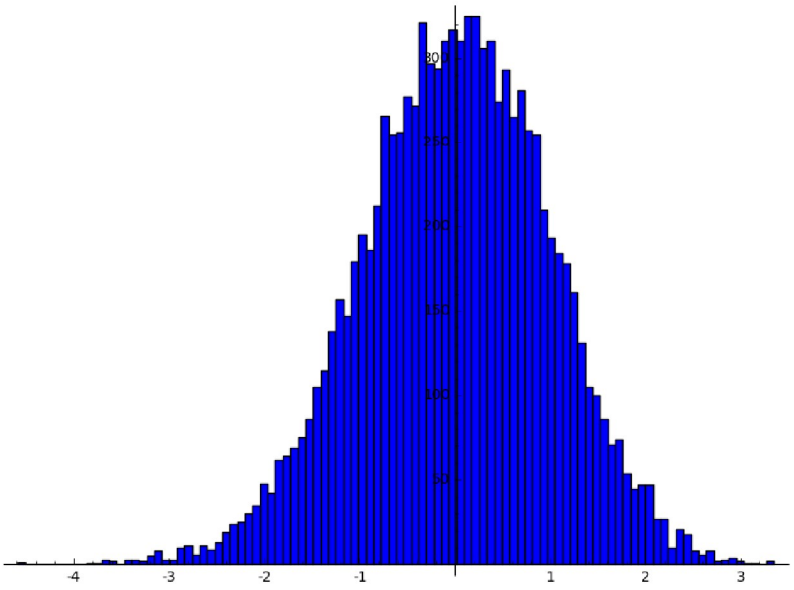
$D_0 = -10^{21}$



$D_0 = -10^{22}$



$D_0 = -10^{23}$



$D_0 = -10^{24}$

Bibliography

[1] D. A. Marcus, *Number fields*, vol. 1995. Springer, 1977.

[2] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, vol. 34. John Wiley & Sons, 2011.

[3] C. Siegel, "Über die classenzahl quadratischer zahlkörper," *Acta Arithmetica*, vol. 1, no. 1, pp. 83–86, 1935.

[4] R. Brauer, "On the zeta-functions of algebraic number fields," *American Journal of Mathematics*, vol. 69, no. 2, pp. 243–250, 1947.

[5] H. Cohen and H. W. Lenstra Jr, "Heuristics on class groups of number fields," in *Number Theory Noordwijkerhout 1983*, pp. 33–62, Springer, 1984.

[6] J. E. Littlewood, "On the class-number of the corpus $p(\sqrt{-k})$," *Proceedings of the London Mathematical Society*, vol. 2, no. 1, pp. 358–372, 1928.

[7] P. Erdős and M. Kac, "The gaussian law of errors in the theory of additive number theoretic functions," *American Journal of Mathematics*, vol. 62, no. 1, pp. 738–742, 1940.

[8] H. H. Nguyen, V. Vu, *et al.*, "Random matrices: Law of the determinant," *The Annals of Probability*, vol. 42, no. 1, pp. 146–167, 2014.

[9] N. Goodman, "The distribution of the determinant of a complex wishart distributed matrix," *The Annals of mathematical statistics*, vol. 34, no. 1, pp. 178–180, 1963.

[10] T. Tao and V. Vu, "On random$\pm$1 matrices: singularity and determinant," *Random Structures & Algorithms*, vol. 28, no. 1, pp. 1–23, 2006.