Counting in number theory

# Counting fields

Carl Pomerance, Dartmouth College

Rademacher Lecture 4, University of Pennsylvania
September, 2010

**Finite fields**: Up to isomorphism, there is exactly one for each prime or prime power.

Let $\pi^*(x)$ denote the number of such in $[1, x]$, and let $\pi(x)$ denote the number of primes.

Since $\pi^*(x) - \pi(x) < \sqrt{x}$, the gap is within the margin of error even assuming the Riemann hypothesis. Thus, we have the excellent approximation

$$\pi^*(x) \approx \mathrm{li}(x) := \int_2^x \frac{dt}{\log t}.$$

We have

$$\begin{aligned}
\pi(10^{23}) &= 1\,925\,320\,391\,606\,803\,968\,923,\\
\pi^*(10^{23}) &= 1\,925\,320\,391\,619\,238\,700\,024,\\
\int_2^{10^{23}} \frac{\mathrm{d}t}{\log t} &= 1\,925\,320\,391\,614\,054\,155\,138.
\end{aligned}$$

As mentioned in Lecture 1, the Riemann Hypothesis is equivalent to

$$|\pi(x) - \mathrm{li}(x)| < \sqrt{x}\log x,$$

for $x \geq 3$. It is also equivalent to

$$|\pi^*(x) - \mathrm{li}(x)| < \sqrt{x}\log x.$$

Say $K$ is an algebraic number field. We know that $K = \mathbb{Q}(\theta)$ for some algebraic integer $\theta$. Let $f(x) \in \mathbb{Z}[x]$ be the minimum polynomial for $\theta$. Note that $(K : \mathbb{Q}) = d$ if and only if $\deg(f) = d$.

So, one way to count (isomorphism classes of) algebraic number fields is to count polynomials. For example, consider all polynomials

$$x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in \mathbb{Z}[x]$$

with each $|a_i| \leq N$. There are $(2N+1)^d$ such polynomials. Some may be reducible. Some may give rise to the same field. But as $N$ increases, we will eventually get to every field.

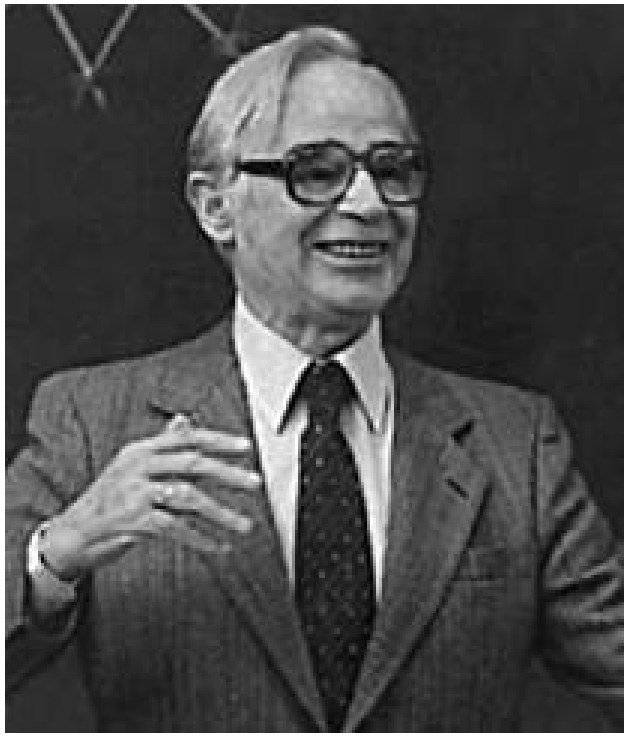
van der Waerden: Most of these polynomials are irreducible, and in fact, most of them give a field $K$ whose normal closure has degree $d!$, that is, the Galois group is $S_d$.

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in \mathbb{Z}[x], \quad |a_i| \le N.$$

van der Waerden: Conjectured that the number of non-$S_d$ choices for $f$ is $O(N^{d-1})$. (Essentially proved when $d = 3$ by Lefton (1979) and in the case $d = 4$ by Dietmann (2006).)

Gallagher (1972): All but $O(N^{d-1/2} \log N)$ choices for $f$ are $S_d$.

Liu & Murty (1999): Found a simple proof but with the weaker exponent $d - 1/3$.



B. L. van der Waerden

Yu-Ru Liu

## Another way to count: discriminants

What is the discriminant?

If $\theta_1, \theta_2, \ldots, \theta_d$ form an integral basis for $K$ over $\mathbb{Q}$ (that is, $\mathcal{O}_K = \mathbb{Z}\theta_1 \bigoplus \mathbb{Z}\theta_2 \bigoplus \cdots \bigoplus \mathbb{Z}\theta_d$, where $\mathcal{O}_K$ is the ring of integers of $K$), then

$$\mathrm{disc}(K) = \det(\sigma_i(\theta_j))^2,$$

where $\sigma_1, \sigma_2, \ldots, \sigma_d$ are the different isomorphisms of $K$ into the complex numbers.

Note that $\mathrm{disc}(K) \in \mathbb{Z}$.

Unlike with counting polynomials, where there are infinitely many polynomials that give the same field, with discriminants, our field $K$ has just one statistic, and it's an integer.

However, there is no confusion with polynomials, as there is a mapping from (irreducible) polynomials to isomorphism classes of fields. With discriminants, we have a mapping from fields to integers, but one integer might be the discriminant of many non-isomorphic fields.

Artin: In 1928 conjectured that non-isomorphic cubic fields have distinct discriminants. (Mentioned in a 1964 paper of Delone & Faddeev.) This perhaps is the natural generalization from quadratic fields.

Scholz & Taussky: In 1934 found four integers which are each discriminants for two non-isomorphic complex cubic fields.

We have since found many other examples, with the record multiplicity being 9.

Ellenberg & Venkatesh: At most $|D|^{1/3+\varepsilon}$ cubic fields can have discriminant $D$.

For more on discriminant multiplicities see the website of Daniel C. Mayer: http://www.algebra.at/index_e.htm

Olga Taussky Todd

Jordan Ellenberg

Akshay Venkatesh

Let $N_d(X)$ denote the number of isomorphism classes of algebraic number fields $K \subset \mathbb{C}$ of degree $d$ over $\mathbb{Q}$ and with $|\text{disc}(K)| \leq X$. (Note that we are counting fields, not discriminants, so we count discriminants with multiplicity.)

Further, if $G$ is a finite group, let $N_d(G, X)$ be the number of such fields $K$ whose normal closure has Galois group isomorphic to $G$. For there to be any such fields $K$, it is necessary that $G$ is a transitive permutation group on $d$ letters.

Is this condition sufficient???

Let's try $d = 2$, quadratic fields. Here there is a one-to-one correspondence with *fundamental discriminants*. (That is, the multiplicity for a discriminant is always 1.)

"fundamental discriminant": squarefree, not 1, and 1 (mod 4) or 4 times a squarefree number that is 2 or 3 (mod 4).

Using what's known about the distribution of squarefree numbers, we have

$$N_2(X) \sim \frac{1}{\zeta(2)} X = \frac{6}{\pi^2} X.$$

One might also ask about real and complex fields separately, that is, positive and negative discriminants. Easy, it's 50-50:

$$N_{2,0}(X) \sim \frac{3}{\pi^2} X, \quad N_{0,1}(X) \sim \frac{3}{\pi^2} X.$$

Let us compare this asymptotic formula for the distribution of quadratic field discriminants with the numerical evidence. For example, for $X = 10^{25}$, we have

$$\begin{aligned} N_{2,0}(X) &= 3\,039\,635\,509\,270\,133\,143\,448\,215, \\ N_{0,1}(X) &= 3\,039\,635\,509\,270\,133\,143\,069\,580, \\ \frac{3}{\pi^2}X &= 3\,039\,635\,509\,270\,133\,143\,316\,384, \end{aligned}$$

(Cohen, Diaz y Diaz, & Olivier). Since the Dirichlet generating function for the squarefree integers is

$$\frac{\zeta(s)}{\zeta(2s)},$$

it is conjectured that the error should be of magnitude $O(X^{1/4})$. The best that's proved is $o(X^{1/2})$ unconditionally and $O(X^{17/54+\varepsilon})$ on RH (Walfisz, Montgomery–Vaughan, Graham, Baker–Pintz, Jia).

Henri Cohen

Now, let's try cubic fields. There are two possible groups for the normal closure: $C_3$, $S_3$.

For $C_3$, Cohn (1954), following work of Hasse (1930), showed that

$$N_3(C_3, X) = cX^{1/2} + O(X^{1/3+\varepsilon}),$$

where

$$c = \frac{11\sqrt{3}}{36\pi} \prod_{p \equiv 1 \pmod 3} \left(1 - \frac{2}{p(p+1)}\right) \approx 0.1585\ldots.$$

By the numbers, for $X = 10^{37}$, we have

$$\begin{aligned} N_3(C_3, X) &= 501\,310\,370\,031\,289\,126, \\ cX^{1/2} &= 501\,310\,370\,031\,520\,350, \end{aligned}$$

(Cohen, Diaz y Diaz, & Olivier). It is conjectured that the error is perhaps $O(X^{1/6})$.

For $S_3$-cubic fields, we have Davenport & Heilbronn (1971):

$$N_{3,0}(X) \sim \frac{1}{12\zeta(3)}X, \quad N_{1,1}(X) \sim \frac{1}{4\zeta(3)}X.$$

Among early efforts to actually tabulate these cubics, we have Fung & Williams (1990, 1994):

$$N_{1,1}(10^6) = 182\,417, \quad \frac{1}{4\zeta(3)}10^6 = 207\,977$$

and Llorente & Quer (1988):

$$N_{3,0}(10^7) = 592\,922, \quad \frac{1}{12\zeta(3)}10^7 = 693\,256.$$

(The count for $N_{3,0}$ includes 501 cyclic cubic fields and has been corrected by $-1$ after Cohen, Diaz y Diaz, & Olivier.)

Harold Davenport

Hans Heilbronn

Concerning the count 182 417 vs. the prediction 207 977, Fung & Williams (1990):

"Davenport and Heilbronn have proved a theorem which says that this density should approach the asymptotic limit of $(4\zeta(3))^{-1} \approx .20798$. If however, the reader were to plot the [empirical] density, he would be somewhat astonished to see that this density is increasing so slowly that his first impression would be that it will not make it to the Davenport–Heilbronn limit. Thus, it remains a challenging problem, assuming the D–H limit is not in error, to explain the origin of this slow convergence. ... [O]n the real side, ... the problem is further aggravated by even slower convergence. To date, and to our knowledge, no good quantitative explanation of this phenomenon has been given."

Well, we've now computed to $10^{11}$ (Belabas 1997):

$$N_{3,0}(X) = 6\,715\,773\,873, \quad N_{1,1}(X) = 20\,422\,230\,540,$$
$$\frac{1}{12\zeta(3)}X = 6\,932\,561\,438, \quad \frac{1}{4\zeta(3)}X = 20\,797\,684\,315.$$

Belabas 1999: The error from the Davenport–Heilbronn main term is at most

$$O\left(X/\exp(\sqrt{\log X})\right).$$

Karim Belabas

David Roberts

Roberts 2000: Conjectured that the error is asymptotically $c'X^{5/6}$, where

$$c' = \frac{4\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)} \approx 0.147685261$$

in the totally real case, and $\sqrt{3}c'$ in the complex case:

$$N_{3,0}(X) \approx \frac{1}{12\zeta(3)}X - c'X^{5/6}, \quad N_{1,1}(X) \approx \frac{1}{4\zeta(3)}X - \sqrt{3}c'X^{5/6}.$$

Looking at the numbers at $X = 10^{11}$:

| | $N_{3,0}(X)$ | $N_{1,1}(X)$ |
|---|---|---|
| actual : | 6 715 773 873, | 20 422 230 540 |
| predicted : | 6 715 789 120, | 20 422 223 646. |

**Theorem** (Belabas, Bhargava, & P 2010):

$$N_{3,0}(X) = \frac{1}{12\zeta(3)}X + O\left(X^{7/8}(\log X)^2\right),$$

$$N_{1,1}(X) = \frac{1}{4\zeta(3)}X + O\left(X^{7/8}(\log X)^2\right).$$

Manjul Bhargava

Let

$$\xi_d(s) = \sum_K |\mathrm{disc}(K)|^{-s},$$

where $K$ runs over the isomorphism classes of number fields of degree $d$. The Davenport–Heilbronn theorem implies that $\xi_3(s)$ is analytic in the region $\Re(s) > 1$. Cohen had asked if it could be continued to a larger region. As a bonus, we have $\xi_3(s)$ analytic for $\Re(s) > 7/8$.

(Shintani:

$$\sum_{[K:\mathbb{Q}]=3} |\mathrm{disc}(K)|^{-s} \frac{\zeta_K(2s)}{\zeta_K(4s)}$$

has a meromorphic extension to $\mathbb{C}$ with the two rightmost poles simple at $s = 1$ and $s = 5/6$.)

And we have an added bonus: using a result of Hasse (1930) that connects cubic orders to the 3-torsion of a quadratic field with the same discriminant, we have

**Theorem** (Belabas, Bhargava, & P 2010):

$$\sum_{0<D\leq X} \#\mathrm{Cl}_3(D) = \frac{4}{\pi^2}X + O\left(X^{7/8+\varepsilon}\right),$$

$$\sum_{-X\leq D<0} \#\mathrm{Cl}_3(D) = \frac{6}{\pi^2}X + O\left(X^{7/8+\varepsilon}\right).$$

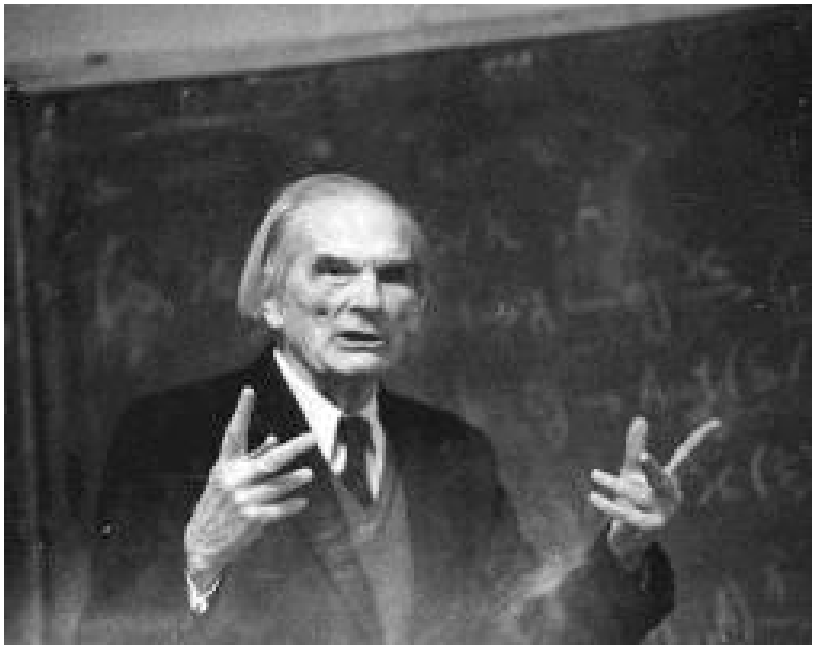
(The main terms were due to Davenport & Heilbronn.)

Our proof rests on the Delone & Faddeev (1964) correspondence:

*There is a natural correspondence between cubic orders up to isomorphism and classes of irreducible binary cubic forms modulo* GL(2,$\mathbb{Z}$)*. The correspondence preserves discriminant and content.*

This result allows us to deal with cubic fields in a very concrete way. But, it is *maximal* orders that correspond naturally to fields, and in the Delone–Faddeev result, we are dealing with all orders.

B. N. Delone



D. K. Faddeev

So, say we start with all cubic orders. A result of Davenport (1951), as improved by Shintani (1972), says that the number of classes of binary cubic forms $f$ with $|\text{disc}(f)| \leq X$ is

$$cX + O(X^{5/6})$$

(actually separate results for positive and negative discriminants). So this is great! A power-saving error term. But we want binary cubic forms corresponding to maximal orders.

So, we try an inclusion-exclusion argument where we count orders $\mathcal{O}$ with $|\text{disc}(\mathcal{O})| \leq X$ which have index in their maximal order divisible by $q$.

Going over to binary cubic forms, and from them to the lattice of coefficients modulo GL(2,$\mathbb{Z}$), we note that having the index of $\mathcal{O}$ divisible by $q$ corresponds to congruence conditions in the lattice modulo $q^2$. Further, the number of these congruence classes is

$$q^8 \prod_{p|q} \left(p^{-2} + p^{-3} - p^{-5}\right) \approx q^6$$

out of the total of $q^8$ classes.

We show that in a particular congruence class that can occur with first coordinate fixed as $a$ mod $q^2$, the count is $q^{-8}$ times the full number of all orders plus the error term

$$O\left(q^{-6}a^{-1/3}X^{5/6} + q^{-4}a^{-2/3}X^{2/3} + \log X\right).$$

We also have an approximate equi-distribution result for the parameter "$a$" (the leading coefficient of the cubic form) among these roughly $q^6$ residue classes. We take a sum of our estimates for the various fixed residue classes. The main term, as mentioned, is about $q^{-2}$ times the full number of lattice points, and the error turns out as

$$O\left(\frac{q}{\varphi(q)}(q^{-2/3}X^{5/6} + q^6 \log X)\right).$$

The major shape of the argument is inclusion-exclusion over the variable $q$. So that we might truncate the process at a reasonable point, we also need a uniform upper bound corresponding to large values of $q$. This can be done via elementary methods.

We've dealt with finite fields, quadratic fields, cubic fields; hmmm, what could be next?

For a quartic field over $\mathbb{Q}$, possible Galois groups for the normal closure are $C_4$, $V_4$, $A_4$, $D_4$, and $S_4$.

The general case when the group is abelian has been considered by many: Khushvaktov (1977), Urazbaev (1977), Baily (1980), Zhang (1984), Mäki (1985), and Wright (1989).

In particular,

$$N_4(C_4, X) = cX^{1/2} + O(X^{1/3+\varepsilon}),$$
$$N_4(V_4, X) = (c_2(\log X)^2 + c_1 \log X + c_0)X^{1/2} + O(X^{1/3+\varepsilon}).$$

These results are also refined by signature. Supported by massive computation, Cohen, Diaz y Diaz, & Olivier (2006) conjecture much smaller error estimates in these counts (but with an explicit $X^{1/3}$-secondary term in the case of $C_4$.)

The case of $A_4$ is not completely solved, but heuristically and numerically, we seem to have $N_4(A_4, X)$ of the shape $X^{1/2} \log X$. Wong (2005) proves $O(X^{5/6+\varepsilon})$.

The case of $D_4$ provides a bit of a surprise. Here, Cohen, Diaz y Diaz, & Olivier (2002) proved that

$$N_4(D_4, X) = cX + O(X^{3/4+\varepsilon}).$$

The constant $c$ is explicit; they suggest in later numerical work a secondary term of shape $X^{1/2}$ with a still-smaller error term.

The main result is surprising because it says that a positive proportion of integers are discriminants of $D_4$-quartic extensions, and supposedly it is $S_4$ that's the generic case!

A folk conjecture, perhaps due to Narkiewicz:

$$N_d(X) \sim c_d X$$

for each integer $d \geq 2$, where $c_d > 0$. This conjecture was refined by Cohen (2000), Malle (2002, 2004), and Bhargava (2007). These refinements suggest that when degree $d$ fields are counted separately by their Galois groups, that those groups which contain a transposition, when viewed as a transitive permutation group on $d$ letters, will contribute a positive proportion to the count. And those groups which do not contain a transposition will contribute at most $O(X^{1/2+\varepsilon})$.

Note that the transitive permutation groups on 4 letters which contain a transposition are precisely $D_4$ and $S_4$, thus "explaining" the surprise.

In his dissertation, Bhargava (2001) found asymptotic formulas of a constant times $X$ for $N_4(S_4, X)$, and recently (2010) did the same for $N_5(S_5, X)$.

In particular, combining his result for $S_4$ with the known results on other quartic fields, one gets that, counted by discriminant, 0.17111 of them are $D_4$ and 0.82889 of them are $S_4$ (with these fractions rounded of course).

The proofs are complicated, but in a nutshell, Bhargava finds analogies for the Delone–Faddeev correspondence for cubic fields. In particular for quartic fields, he considers pairs of ternary quadratic forms modulo GL(2,$\mathbb{Z}$)×SL(3,$\mathbb{Z}$). And for quintics, he considers quadruples of alternating bilinear forms in five variables modulo the action of GL(4,$\mathbb{Z}$)×SL(5,$\mathbb{Z}$).

The numbers for $S_4$-quartic fields are not too convincing. They are difficult to compute, and for all signatures they have only been enumerated up to $X = 10^7$. At this level, the actual and predicted counts are

$$1\,635\,308, \qquad 2\,534\,771$$

(exact count by Cohen, Diaz y Diaz, & Olivier (2006)).

Malle has continued the count to $10^9$ in the totally real case, and at that level, the actual vs. predicted counts are

$$17\,895\,702, \qquad 25\,347\,714.$$

Perhaps there is a secondary term of magnitude $X^{7/8}$?

Belabas, Bhargava, & P (2010):

$$N_4(S_4, X) = \frac{5}{24} \prod_p \left(1 + p^{-2} - p^{-3} - p^{-4}\right) X + O\left(X^{23/24+\varepsilon}\right),$$

with natural refinements for the 3 possible signatures.

We have a class number bonus here too. Heilbronn (1971) showed that for a given noncyclic cubic field $K_3$, the number of $S_4$-quartic fields which have cubic resolvent field isomorphic to $K_3$ is $\#\mathrm{Cl}_2(K_3) - 1$. So, we prove that

$$\sum_{0<\mathrm{disc}(K_3)\le X} \#\mathrm{Cl}_2(K_3) = \frac{5}{4} \sum_{0<\mathrm{disc}(K_3)\le X} 1 + O(X^{23/24+\varepsilon}),$$

$$\sum_{0>\mathrm{disc}(K_3)\ge -X} \#\mathrm{Cl}_2(K_3) = \frac{3}{2} \sum_{0>\mathrm{disc}(K_3)\ge -X} 1 + O(X^{23/24+\varepsilon}).$$

Our proofs are similar, but more complicated. Playing the role of "$a$" in the prior argument for cubic fields (it was the leading coefficient of the binary cubic form) we now have four actors, named $a, b, c, d$. These are the coefficients of $x^2, xy, xz, y^2$, respectively, in the first of the two ternary quadratic forms.

Our result counting the number of quartic orders with index divisible by $q$ and with first four coefficients given by $a, b, c, d$ has a simple main term, but the error term is computed from 4094 different 4-fold multiple integrals. Luckily only 33 of these are dominant, and only 3 are critical. The moral: Though the plan is the same simple inclusion-exclusion, the execution of the plan was not easy!

It remains to be seen if Bhargava's $S_5$ work can also be redone with a power-saving error term.

A very interesting avenue for further research is to use the very concrete way we have of asymptotically counting fields to form an algorithm that counts them exactly up to interesting levels. It was such counts in the cubic case that led Roberts to his conjecture on a possible secondary term in the cubic case.

New work of Yang (Ph.D. thesis, Princeton, 2009) applies our results to study the distribution of low-lying zeroes in families of Dedekind zeta functions corresponding to cubic and quartic fields, and so partially verifies a conjecture of Katz & Sarnak about this distribution.

Late breaking news!

The Roberts conjecture for cubic fields has been proved.
Twice.

By Bhargava, Shankar, & Tsimerman and by Thorne.

Arul Shankar

Jacob Tsimerman

Frank Thorne

There is also a sensational new result by Bhargava & Shankar on the average rank of an elliptic curve over $\mathbb{Q}$, using not totally unrelated tools. But perhaps that is a topic for another lecture, and another lecturer.

# THANK YOU!