On Torsion Subgroups in Class Groups of Number Fields

Lillian B. Pierce

At the turn of the 19th century, Gauss was interested in the problem of representation by quadratic forms. The germ of this problem can be traced back as far as Diophantus, nearly 2000 years ago. But let us start for concreteness with a statement by Fermat around the middle of the 17th century that an odd prime can be written as a sum of two squares if and only if it is congruent to 1 modulo 4. Since the square of an integer is either congruent to 0 or 1 modulo 4, the "only if" part of this claim is simple to prove, but the "if" part is more tricky. It was one hundred years after Fermat's statement that Euler provided a proof, and the problem then came to be situated within a broader setting: studying when an integer m is represented by a binary quadratic form $Q(x,y) = ax^2 + bxy + cy^2$, that is, whether there exist integer solutions x, y to the equation $Q(x,y) = m$.

In fact, it is natural to sort binary quadratic forms by discriminant ($b^2 - 4ac$ in this notation). Then one can ask: given an integer m, is there a form of discriminant D that represents m? If so, which forms of discriminant D represent m? Twenty-five years after Euler, Lagrange gave an answer to the first, simpler question: one simply needs to test whether D is a quadratic residue modulo $4m$, that is, whether there exists an integer x such that $D \equiv x^2$ modulo $4m$. But this left open the question of *which* forms of discriminant D represent m, and here is where Gauss took up the problem.

Gauss clarified that you can dissect the set of forms of discriminant D into equivalence classes under $\mathrm{SL}_2(\mathbb{Z})$ changes of variable; forms in the same equivalence class represent the same integers. Moreover, for each D there are finitely many such equivalence classes; the number of such classes is the class number associated to D. The question is now which (if any) equivalence classes of forms of discriminant D represent m?

Given $D < 0$, Gauss constructed a finite set of test functions (real characters with moduli determined by the prime divisors of D), and showed how to use these test functions to create a "fingerprint" for each quadratic form of discriminant D (by evaluating the characters at an integer represented by the form). If there are t test functions, this fingerprint is a sequence of t values of $+1, -1$ whose product is $+1$. Forms in the same equivalence class have the same fingerprint. But it can also happen that different equivalence classes may have the same fingerprint.

Gauss called these new coarser clusters, comprised of forms sharing a fingerprint, the genera of the discriminant D. He showed that there are 2^{t-1} distinct genera, and each genus contains the same number of equivalence classes; hence we arrive at the remarkable fact that 2^{t-1} must divide the class number. How big is t? It turns out that t is the number of distinct prime divisors of D (here for simplicity we assume D is a fundamental discriminant, which means it is square-free, up to certain powers of 2). Gauss had revealed (one might say accidentally) a remarkably simple criterion for when the class number of D is divisible by powers of 2. (The case $D > 0$ is similar.)

In terms of studying the divisibility properties of class numbers, this is the worm that opened the can. (Although it left open the representation question—we know how to test which genera represent a given integer m, but still not which equivalence class or classes within a genus represent m. If we think about the collection of genera as a nest of eggs, and each equivalence class as a yolk, the ambiguity arises when each of the eggs has more than one yolk.)

What about divisibility of the class number by 3? by 5? We still don't understand these questions nearly as well. Even questions about the size of class numbers remain difficult. Gauss did a remarkable number of computations by hand (for example computing the class number for each discriminant between $-9,000$ and $-10,000$), which led to beautiful predictions, such as that there should only be finitely many $D < 0$ with a given class number, while there should be infinitely many $D > 0$ with class number 1. Alongside his predictions, he remarked, "Demonstrationes autem *rigorosae* harum observationum perdifficiles esse videntur."[1] Among the many things that Gauss was right about, he seems to have been right about this; celebrated work has shown the first statement to be true, while the second remains a mystery.

In modern terms, Gauss was studying the class group (with cardinality being the class number) of quadratic fields $\mathbb{Q}(\sqrt{D})$, for a positive or negative integer D. More generally, given any finite degree field extension K of $\mathbb{Q}$, we can study the class group Cl_K, which is defined to be the quotient group of the fractional ideals of the ring of integers of K by the principal ideals. In each case, the class group Cl_K is a finite abelian group, whose cardinality is called the class number. Class groups are central objects in number

Lillian B. Pierce is an associate professor of mathematics at Duke University. Her email address is pierce@math.duke.edu.

DOI: https://doi.org/10.1090/noti/1777

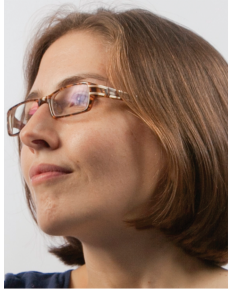
[1] *Translated in* [GSS07, p.13] *as "However, rigorous proofs of these observations appear to be difficult."*

theory, and questions about the divisibility properties of class numbers fit into a broader theme of questions about the structure of class groups of fields as the fields vary over a family of interest.

This talk will focus on the size of torsion subgroups in class groups. If we fix a prime ℓ, how many elements of order ℓ (ℓ-torsion elements) can exist in a class group Cl_K for a particular field K? Can we learn more if we work on average as K varies over an appropriately defined family of fields? This talk will survey recent progress on these questions, and how they relate to other well-known conjectures in number theory, such as fundamental questions on counting number fields.

References

[GSS07] Catherine Goldstein, Norbert Schappacher, and Joachim Schwermer, *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*. Springer–Verlag, 2007. MR2308276



Lillian B. Pierce

Credits

Author photo is courtesy of Lillian B. Pierce.