IDEAL CLASSES AND THE KRONECKER BOUND

KEITH CONRAD

1. Introduction

Let A be a domain with fraction field F. A *fractional A-ideal* is a nonzero A-submodule $\mathfrak{a} \subset F$ such that $d\mathfrak{a} \subset A$ for some nonzero $d \in A$. These are the nonzero ideals in A divided by elements of $F^\times$. Principal fractional A-ideals are $(x) := xA$ for $x \in F^\times$. We call a fractional A-ideal $\mathfrak{a}$ *invertible* if there a fractional A-ideal $\mathfrak{b}$ such that $\mathfrak{ab} = A$.

Call two fractional A-ideals $\mathfrak{a}$ and $\mathfrak{a}'$ equivalent when they are related by scaling: $\mathfrak{a} = x\mathfrak{a}'$ for some $x \in F^\times$. Write this as $\mathfrak{a} \sim \mathfrak{a}'$. The equivalence class of $\mathfrak{a}$ (the set of all $x\mathfrak{a}$ for $x \in F^\times$) is called the *ideal class* of $\mathfrak{a}$ and we write it as $[\mathfrak{a}]$, so $[\mathfrak{a}] = [\mathfrak{a}']$ is the same thing as $\mathfrak{a} \sim \mathfrak{a}'$. The principal fractional A-ideals form a single ideal class, namely $[(1)] = [A]$. Every ideal class is represented by a nonzero ideal in A since we can write any fractional A-ideal as $\frac{1}{d}I$ for some nonzero ideal I in A, and $\frac{1}{d}I \sim I$. An ideal in A is equivalent to (1) if and only if it is a principal ideal: if $\mathfrak{a} \subset A$ and $\mathfrak{a} = xA$ for some $x \in F^\times$ then $x \in xA = \mathfrak{a} \subset A$.

Since $xAyA = xyA$, it is well-defined to multiply ideal classes by multiplying representatives: $[\mathfrak{a}][\mathfrak{a}'] = [\mathfrak{a}\mathfrak{a}']$. Multiplication of ideal classes is obviously commutative and associative, with identity $[(1)] = [A]$, which will usually be written just as 1. We call an ideal class $[\mathfrak{a}]$ invertible if it can be multiplied by an ideal class to have product 1. Then $[\mathfrak{a}]$ is an invertible ideal class if and only if $\mathfrak{a}$ is an invertible fractional A-ideal. In one direction, if $\mathfrak{ab} = A$ then $[\mathfrak{a}][\mathfrak{b}] = 1$. In the other direction, if $[\mathfrak{a}][\mathfrak{b}] = 1$ for some ideal class $[\mathfrak{b}]$ then $\mathfrak{ab}$ is a principal fractional A-ideal, say $\mathfrak{ab} = xA$ for some $x \in F^\times$, and then $\mathfrak{a} \cdot \frac{1}{x}\mathfrak{b} = A$.

Theorem 1.1. *The ideal classes of fractional ideals in a number field form a group.*

Proof. All fractional ideals in a number field are invertible. □

For some integral domains not all fractional ideals are invertible, so not all ideal classes are invertible.

Example 1.2. In $\mathbf{Z}[\sqrt{5}]$, let $\mathfrak{p} = (2, 1 + \sqrt{5})$. This is a prime ideal (index 2 in $\mathbf{Z}[\sqrt{5}]$) and $\mathfrak{p}^2 = 2\mathfrak{p}$, so $\mathfrak{p}^2 \sim \mathfrak{p}$. Thus $[\mathfrak{p}]^2 = [\mathfrak{p}]$. If $[\mathfrak{p}]$ had an inverse, then $\mathfrak{p}$ would have an inverse as a fractional $\mathbf{Z}[\sqrt{5}]$-ideal, so the equation $\mathfrak{p}^2 = 2\mathfrak{p}$ would imply $\mathfrak{p} = (2)$ by cancellation. But $\mathfrak{p}$ has index 2 in $\mathbf{Z}[\sqrt{5}]$ while (2) has index 4, so $\mathfrak{p} \neq (2)$.

The ideal classes of $\mathbf{Z}[\sqrt{5}]$ are not a group and can't be embedded in a group, since Example 1.2 shows there would be a contradiction if $[\mathfrak{p}]$ becomes invertible somehow.

We call the ideal classes of fractional ideals in a number field K the *ideal class group* of K or just the *class group* of K, and write it as $\mathrm{Cl}(K)$. The elements of this group are the ideal classes $[\mathfrak{a}] = \{x\mathfrak{a} : x \in K\}$, with the group law being multiplication of representatives. The group $\mathrm{Cl}(K)$ is abelian, and this group is trivial if and only if all fractional ideals in K are principal, which is equivalent to $\mathcal{O}_K$ being a PID. Ideal class groups of number fields are fundamental objects in number theory. We will prove the ideal class group of every number

field is finite, describe how to calculate some examples of ideal class groups, and mention some open questions about the size of ideal class groups of number fields.

2. Finiteness

Theorem 2.1. *Every number field K has a finite ideal class group. That is, there are a finite number of fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ in K such that every fractional ideal is $x\mathfrak{a}_i$ for some $x \in K^\times$.*

Proof. The argument has two steps.

Step 1. There is a constant $C > 0$ such that in every nonzero ideal $\mathfrak{a} \subset \mathcal{O}_K$ there is a nonzero α such that $\left|\mathrm{N}_{K/\mathbf{Q}}(\alpha)\right| \leqslant C[\mathcal{O}_K : \mathfrak{a}]$.

(For nonzero $\alpha \in \mathfrak{a}$ we have $(\alpha) \subset \mathfrak{a} \subset \mathcal{O}_K$, so $\left|\mathrm{N}_{K/\mathbf{Q}}(\alpha)\right| = [\mathcal{O}_K : (\alpha)] \geqslant [\mathcal{O}_K : \mathfrak{a}]$. Thus we are saying this inequality can be reversed for some α in $\mathfrak{a}$ at the cost of introducing a constant C that is independent of the choice of $\mathfrak{a}$.)

The constant C will depend on a choice of $\mathbf{Z}$-basis of $\mathcal{O}_K$. Write $n = [K : \mathbf{Q}]$ and $\mathcal{O}_K = \mathbf{Z}e_1 \oplus \cdots \oplus \mathbf{Z}e_n$. We will use embeddings of K into the complex numbers, and make *estimates* with these embeddings. There are n field embeddings

$$\sigma_1, \ldots, \sigma_n \colon K \to \mathbf{C},$$

and the norm map $\mathrm{N}_{K/\mathbf{Q}}$ can be expressed in terms of them: for each $x \in K$,

$$\mathrm{N}_{K/\mathbf{Q}}(x) = \sigma_1(x)\sigma_2(x)\cdots\sigma_n(x). \tag{1}$$

Writing $x = c_1e_1 + \cdots + c_ne_n$ with $c_i \in \mathbf{Q}$, we get

$$\begin{aligned}
\left|\mathrm{N}_{K/\mathbf{Q}}(x)\right| &= \prod_{j=1}^{n} |\sigma_j(x)| \\
&= \prod_{j=1}^{n} \left| \sum_{i=1}^{n} c_i \sigma_j(e_i) \right| \\
&\leqslant \prod_{j=1}^{n} \Big(\sum_{i=1}^{n} |c_i| \, |\sigma_j(e_i)| \Big) \\
&\leqslant \big(\max |c_i|\big)^n \underbrace{\prod_{j=1}^{n} \Big(\sum_{i=1}^{n} |\sigma_j(e_i)| \Big)}_{\text{Call this } C}.
\end{aligned}$$

For any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, its index in $\mathcal{O}_K$ lies between nth powers of consecutive integers, say $k^n \leqslant [\mathcal{O}_K : \mathfrak{a}] < (k+1)^n$. The set

$$\Big\{ \sum_{i=1}^{n} a_i e_i : a_i \in \mathbf{Z},\ 0 \leqslant a_i \leqslant k \Big\}$$

has size $(k+1)^n$, so by the pigeonhole principle we have

$$\sum_{i=1}^{n} a_i e_i \equiv \sum_{i=1}^{n} a_i' e_i \bmod \mathfrak{a},$$

where $0 \leqslant a_i, a_i' \leqslant k$ and $a_i \neq a_i'$ for some i. Taking the difference $c_i = a_i - a_i'$,

$$\sum_{i=1}^{n} c_i e_i \in \mathfrak{a},$$

and $|c_i| \leqslant k$ with $c_i \neq 0$ for some i. Call this sum α. Then $\alpha \neq 0$ and

$$\left|\mathrm{N}_{K/\mathbf{Q}}(\alpha)\right| \leqslant \left(\max|c_i|\right)^n C \leqslant k^n C \leqslant [\mathcal{O}_K : \mathfrak{a}]C.$$

Step 2. (Finiteness)

Every fractional ideal class is represented by a nonzero ideal $\mathfrak{a} \subset \mathcal{O}_K$. Pick nonzero α in $\mathfrak{a}$ such that

$$\left|\mathrm{N}_{K/\mathbf{Q}}(\alpha)\right| \leqslant C[\mathcal{O}_K : \mathfrak{a}] \tag{2}$$

by Step 1. Since $\left|\mathrm{N}_{K/\mathbf{Q}}(\alpha)\right| = [\mathcal{O}_K : \alpha\mathcal{O}_K]$ and $\alpha\mathcal{O}_K \subset \mathfrak{a} \subset \mathcal{O}_K$, the inequality (2) is equivalent to $[\mathfrak{a} : \alpha\mathcal{O}_K] \leqslant C$. So $[\frac{1}{\alpha}\mathfrak{a} : \mathcal{O}_K] \leqslant C$. Thus every fractional ideal class is represented by a fractional ideal $\frac{1}{\alpha}\mathfrak{a}$ that *contains* $\mathcal{O}_K$ with index bounded above independently of the ideal class.

To prove there are finitely many ideal classes, it suffices to show for each $r \in \mathbf{Z}^+$ that there are finitely many fractional ideals $\mathfrak{a}$ in K containing $\mathcal{O}_K$ with index r. If $\mathcal{O}_K \subset \mathfrak{a}$ and $[\mathfrak{a} : \mathcal{O}_K] = r$, then $r\mathfrak{a} \subset \mathcal{O}_K$, so $\mathcal{O}_K \subset \mathfrak{a} \subset \frac{1}{r}\mathcal{O}_K$. Since $[\frac{1}{r}\mathcal{O}_K : \mathcal{O}_K] = r^n$, $\frac{1}{r}\mathcal{O}_K/\mathcal{O}_K$ is finite, so there are finitely many such $\mathfrak{a}$. We're done. □

The proof of Theorem 2.1 tells us the ideal classes in $\mathrm{Cl}(K)$ are represented by fractional ideals $\mathfrak{a}$ such that $\mathcal{O}_K \subset \mathfrak{a}$ and $[\mathfrak{a} : \mathcal{O}_K] \leqslant C$, where

$$C = \prod_{\sigma\colon K \to \mathbf{C}} \sum_{i=1}^{n} |\sigma(e_i)|$$

for some choice of $\mathbf{Z}$-basis $\{e_1, \ldots, e_n\}$ of $\mathcal{O}_K$. That doesn't mean C is a bound on the number of ideal classes; it is a bound on the index with which some fractional ideal in each ideal class contains $\mathcal{O}_K$. There could be several fractional ideals containing $\mathcal{O}_K$ with the same index, but there are only a finite number of them.

We will call C the *Kronecker bound* since it essentially occurs in Kronecker's thesis [13, p. 15] in the special case of $\mathbf{Q}(\zeta_p)$ and Kronecker pointed out in another paper later [12, pp. 64–65] that the argument using this bound applies to any number field.

Counting fractional ideals that contain $\mathcal{O}_K$ with a given index might feel a bit strange compared to counting ideals inside $\mathcal{O}_K$ with a given index. Using inversion, we will pass to the second point of view.

Theorem 2.2. *The ideal classes of $\mathcal{O}_K$ are*

- *represented by ideals in $\mathcal{O}_K$ with norm at most C,*
- *generated as a group by prime ideals $\mathfrak{p}$ with $\mathrm{N}(\mathfrak{p}) \leqslant C$.*

Proof. We already know the ideal classes are represented by fractional ideals $\mathfrak{a}$ where $\mathcal{O}_K \subset \mathfrak{a}$ and $[\mathfrak{a} : \mathcal{O}_K] \leqslant C$. Write the condition $\mathcal{O}_K \subset \mathfrak{a}$ as $\mathfrak{a}^{-1} \subset \mathcal{O}_K$. We will show $[\mathcal{O}_K : \mathfrak{a}^{-1}] = [\mathfrak{a} : \mathcal{O}_K]$, so inversion exchanges the fractional ideals containing $\mathcal{O}_K$ with index at most C and the ideals contained in $\mathcal{O}_K$ with index (norm) at most C.

Write $\mathfrak{a}^{-1} = \mathfrak{b}$, which is an ideal in $\mathcal{O}_K$, and write $\mathfrak{a} = \frac{1}{a}\mathfrak{c}$ for $a \in \mathcal{O}_K$ and $\mathfrak{c} \subset \mathcal{O}_K$. Then $(a) = \mathfrak{b}\mathfrak{c}$, so $\mathrm{N}((a)) = \mathrm{N}(\mathfrak{b})\,\mathrm{N}(\mathfrak{c})$ and $[\mathfrak{a} : \mathcal{O}_K] = [\frac{1}{a}\mathfrak{c} : \mathcal{O}_K] = [\mathfrak{c} : a\mathcal{O}_K] = \mathrm{N}((a))/\mathrm{N}(\mathfrak{c}) = \mathrm{N}(\mathfrak{b}) = [\mathcal{O}_K : \mathfrak{b}] = [\mathcal{O}_K : \mathfrak{a}^{-1}]$.

Ideals in $\mathcal{O}_K$ with norm at most C are products of prime ideals with norm at most C, so the ideal classes of such primes generate $\mathrm{Cl}(K)$. □

Just like $\mathcal{O}_K$, the ideal classes of a Dedekind domain A form a group since all fractional A-ideals are invertible. The group of ideal classes of fractional A-ideals is called the ideal class group of A and is written as $\mathrm{Cl}(A)$, so what we wrote before as $\mathrm{Cl}(K)$ for number fields K is $\mathrm{Cl}(\mathcal{O}_K)$ in this notation. While the ring of integers of a number field has a finite ideal class group, other Dedekind domains can have an infinite ideal class group. For example, the ideal class group of $\mathbf{C}[X, \sqrt{X^3 - X}]$ (which is integrally closed) turns out to be isomorphic to the torus $\mathbf{C}/(\mathbf{Z}+\mathbf{Z}i)$. In a sense, the "reason" ideal class groups of number fields are finite is that $\mathbf{Z}/m\mathbf{Z}$ is finite for $m \neq 0$; we did use that finiteness in the proof of Theorem 2.1. To justify this idea, when $\mathbf{F}$ is a finite field the integral closure of $\mathbf{F}[x]$ in a finite extension of $\mathbf{F}(x)$ has a finite ideal class group and the proof of that uses finiteness of $\mathbf{F}[x]/(f(x))$ for nonzero $f(x)$.

For a Dedekind domain A, the group $\mathrm{Cl}(A)$ is trivial if and only if A is a PID, which is equivalent to A being a UFD, so $\mathrm{Cl}(A)$ is a measure of how far A is from having unique factorization of elements. The ideal class group is abelian, and a theorem of Claborn [5, pp. 219–222] says every abelian group is the ideal class group of some Dedekind domain. (See [6] for a refinement on the type of Dedekind domain that is needed.) It is believed that every finite abelian group is the class group of some number field, but this is still unsolved.

Since $x\mathfrak{a} = xA \cdot \mathfrak{a}$ and the principal fractional A-ideals form a group under multiplication ($xA \cdot yA = xyA$ and $(xA)^{-1} = \frac{1}{x}A$), we can think about ideal classes as cosets for the subgroup of principal fractional A-ideals. Therefore when A is Dedekind, $\mathrm{Cl}(A)$ can be regarded as a quotient group

$$\mathrm{Cl}(A) = \{\text{fractional } A\text{-ideals}\} \,/\, \{\text{principal fractional } A\text{-ideals}\}. \tag{3}$$

In every Dedekind domain all fractional ideals are invertible. It turns out that the converse is true as well. This will be a consequence of the next two lemmas.

Let A be a domain with fraction field F. For any two A-modules M and N in F (these modules are not assumed to be finitely generated), we define their product to be the A-module

$$MN := \Big\{ \sum_{i=1}^{r} x_i y_i : r \geqslant 1,\ x_i \in M,\ y_i \in N \Big\}.$$

The identity for this multiplication is A. Invertibility for this multiplication has a built-in finiteness:

Lemma 2.3. *If $MN = A$ then M and N are finitely generated.*

Proof. Some *finite* sum of products is equal to 1: $x_1x_1' + \cdots + x_kx_k' = 1$ where $x_i \in M$ and $x_i' \in N$. For any $x \in M$,

$$x = 1 \cdot x = x_1(x_1'x) + \cdots + x_k(x_k'x),$$

and $x_i'x \in NM = A$, so $M \subset \sum_{i=1}^k Ax_i \subset M$. Thus $M = \sum_{i=1}^k Ax_i$. Similarly, $N = \sum_{i=1}^k Ax_i'$. □

A finitely generated A-module in F certainly has a common denominator, so Lemma 2.3 tells us that invertible A-modules in F are automatically fractional A-ideals.

Lemma 2.4. *If a domain has cancellation of ideals, i.e., always $\mathfrak{ac} = \mathfrak{bc}$ implies $\mathfrak{a} = \mathfrak{b}$ when $\mathfrak{c} \neq (0)$, then the domain is integrally closed.*

Proof. Let A be a domain with cancellation of ideals. Suppose an element x in the fraction field of A is integral over A. We want to show x is in A. Write $x = a/b$ where a and b are in A with $b \neq 0$. Since x is integral over A,

$$x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 = 0$$

with $n \geqslant 1$ and $c_i \in A$. Let $R = A[x] = A + Ax + \cdots + Ax^{n-1}$. This is a ring and a nonzero A-module in the fraction field of A. Since x has denominator b, by the definition of R we have $b^{n-1}R \subset A$, so R has common denominator b^{n-1}. Therefore

$$\mathfrak{a} := b^{n-1}R = Ab^{n-1} + Ab^{n-2}a + \cdots + Aa^{n-1}$$

is a nonzero A-module in A, *i.e.*, $\mathfrak{a}$ is a nonzero ideal in A. Since R is a ring, $R^2 = R$, so $\mathfrak{a}^2 = b^{2(n-1)}R^2 = b^{n-1}b^{n-1}R = (b)^{n-1}\mathfrak{a}$. Therefore by cancellation of nonzero ideals in A, $\mathfrak{a} = (b)^{n-1} = b^{n-1}A$, so $b^{n-1}R = b^{n-1}A$. This implies $R = A$, so $x \in R = A$. □

Theorem 2.5. *If all ideal classes for a domain are invertible, then the domain is a Dedekind domain.*

Proof. Let A be the domain. The hypothesis is equivalent to saying all nonzero ideals in A are invertible as fractional A-ideals. By Lemma 2.3, all ideals in A are finitely generated, so A is Noetherian. Invertible ideals can be cancelled, so Lemma 2.4 tells us that A is integrally closed. It remains to show that any nonzero prime ideal $\mathfrak{p}$ is maximal.

Suppose $\mathfrak{p} \subset \mathfrak{a} \subset A$. Then $\mathfrak{p}\mathfrak{a}^{-1} \subset A$, so $\mathfrak{p}\mathfrak{a}^{-1}$ is an ideal and $\mathfrak{p} = \mathfrak{p}\mathfrak{a}^{-1} \cdot \mathfrak{a}$. Since $\mathfrak{p}$ is a prime ideal, it follows that $\mathfrak{p} \supset \mathfrak{p}\mathfrak{a}^{-1}$ or $\mathfrak{p} \supset \mathfrak{a}$. The first condition implies $\mathfrak{p}\mathfrak{a} = \mathfrak{p}$ and the second condition implies $\mathfrak{p} = \mathfrak{a}$. Therefore by cancellation $\mathfrak{a}$ is A or $\mathfrak{p}$, so $\mathfrak{p}$ is maximal. □

For domains like $\mathbf{Z}[\sqrt{5}]$ that are not Dedekind domains, the set of all their ideal classes under multiplication is just a monoid ("group without inverses"). We can get a group by focusing on the invertible ideal classes. For a domain A, its ideal class group $\mathrm{Cl}(A)$ is, by definition, the group of its invertible ideal classes where the group law is multiplication of ideal classes and $[(1)]$ is the identity. Equivalently,

$$\mathrm{Cl}(A) = \{\text{invertible fractional } A\text{-ideals}\} \,/\, \{\text{principal fractional } A\text{-ideals}\}.$$

Compare this with the definition (3) where A is Dedekind.

3. Ideal Classes for $\mathbf{Q}(\sqrt{-5})$

As an example of a class group computation, we will show $\mathbf{Q}(\sqrt{-5})$ has two ideal classes.

Theorem 3.1. *The ideal class group of $\mathbf{Q}(\sqrt{-5})$ has order two.*

Proof. Use $\{e_1, e_2\} = \{1, \sqrt{-5}\}$. Since

$$C = (|e_1| + |e_2|)(|\overline{e_1}| + |\overline{e_2}|) = (1 + \sqrt{5})^2 \approx 10.4,$$

Theorem 2.2 says the group $\mathrm{Cl}(\mathbf{Q}(\sqrt{-5}))$ is

- represented by $\mathfrak{a} \subset \mathbf{Z}[\sqrt{-5}]$ such that $\mathrm{N}(\mathfrak{a}) \leqslant 10$,
- generated by primes $\mathfrak{p}$ with $\mathrm{N}(\mathfrak{p}) \leqslant 10$.

Let's find all such $\mathfrak{p}$.

If $\mathrm{N}(\mathfrak{p}) \leqslant 10$, then $\mathfrak{p}$ divides (2), (3), (5), or (7). These primes decompose as

$$(2) = \mathfrak{p}_2^2,\ (3) = \mathfrak{p}_3\mathfrak{p}_3',\ (5) = (\sqrt{-5})^2,\ (7) = \mathfrak{p}_7\mathfrak{p}_7'.$$

In particular, $\mathfrak{p}_2$ is the unique prime factor of (2).

In $\mathrm{Cl}(\mathbf{Q}(\sqrt{-5}))$ principal ideals become trivial, so

$$[\mathfrak{p}_2]^2 = 1,\ [\mathfrak{p}_3][\mathfrak{p}_3'] = 1,\ [\mathfrak{p}_7][\mathfrak{p}_7'] = 1.$$

Thus $\mathrm{Cl}(\mathbf{Q}(\sqrt{-5}))$ is generated by $\mathfrak{p}_2$, either prime ideal of norm 3, and either prime ideal of norm 7. Since $(1+\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_3$ and $(3+\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_7$, $[\mathfrak{p}_3]$ and $[\mathfrak{p}_7]$ both equal $[\mathfrak{p}_2]^{-1}$. Thus $\mathrm{Cl}(\mathbf{Q}(\sqrt{-5})) = \langle[\mathfrak{p}_2]\rangle$. Since $\mathfrak{p}_2$ is not principal (no principal ideal has index 2) and its square is principal, $[\mathfrak{p}_2]$ has order 2 and thus $\mathrm{Cl}(\mathbf{Q}(\sqrt{-5})) \cong \mathbf{Z}/2\mathbf{Z}$. □

Two consequences of this, for any nonzero ideal $\mathfrak{a}$ in $\mathbf{Z}[\sqrt{-5}]$, are

- $\mathfrak{a}^2$ is principal since $[\mathfrak{a}]^2 = 1$.
- either $\mathfrak{a}$ is principal or $[\mathfrak{a}] = [\mathfrak{p}_2]$, in which case $[\mathfrak{a}\mathfrak{p}_2] = [\mathfrak{a}][\mathfrak{p}_2] = [\mathfrak{p}_2]^2 = 1$, so $\mathfrak{a}\mathfrak{p}_2$ is principal.

Fermat proved for prime p that $-1 \equiv \square \bmod p \iff p = x^2 + y^2$ for some integers x and y. It is not true that $-5 \equiv \square \bmod p \iff p = x^2 + 5y^2$ for some integers x and y, since for instance $-5 \equiv 1 \bmod 3$ and $-5 \equiv 9 \bmod 7$, but 3 and 7 do not have the form $x^2 + 5y^2$. Here is the correct result in this direction, which Fermat had discovered experimentally.

Theorem 3.2. *For a prime number p, $-5 \equiv \square \bmod p \iff p$ or $2p$ has the form $x^2 + 5y^2$ for some integers x and y, and we can't have both p and $2p$ of that form.*

In terms of the examples preceding this theorem, $2 \cdot 3 = 1^2 + 5 \cdot 1^2$ and $2 \cdot 7 = 3^2 + 5 \cdot 1^2$.

Proof. First we will show

$$-5 \equiv \square \bmod p \iff (p) = \mathfrak{p}\mathfrak{p}', \tag{4}$$

where $\mathfrak{p}$ and $\mathfrak{p}'$ are (possibly equal) prime ideals in $\mathbf{Z}[\sqrt{-5}]$.

Having $-5 \equiv \square \bmod p$ is the same thing as $T^2 + 5 \bmod p$ having a nontrivial factorization, and by Kummer's factorization theorem that is the same as (p) having a nontrivial factorization in $\mathbf{Z}[\sqrt{-5}]$, which must be $\mathfrak{p}\mathfrak{p}'$ since $\mathrm{N}((p)) = p^2$. That settles (4).

(Here is an alternate proof of ($\Rightarrow$) in (4) in the standard way one shows $-1 \equiv \square \bmod p$ if and only if $p = x^2 + y^2$ using arithmetic in $\mathbf{Z}[i]$. If $-5 \equiv c^2 \bmod p$, then $p \mid (c^2 + 5)$, so $p \mid (c+\sqrt{-5})(c-\sqrt{-5})$. As ideals in $\mathbf{Z}[\sqrt{-5}]$, we get $(p) \mid (c+\sqrt{-5})(c-\sqrt{-5})$. If (p) were a prime ideal then $(p) \mid (c+\sqrt{-5})$ or $(p) \mid (c-\sqrt{-5})$, so $(p) \mid (c \pm \sqrt{-5})$ for some choice of sign. Therefore $p \mid (c \pm \sqrt{-5})$ as numbers, so $p \mid \pm 1$ in $\mathbf{Z}$, a contradiction. This shows the ideal (p) is not prime. Since $\mathrm{N}((p)) = p^2$, the nontrivial factorization of (p) must be $\mathfrak{p}\mathfrak{p}'$ where $\mathfrak{p}$ and $\mathfrak{p}'$ have norm p.

An alternate proof of ($\Leftarrow$) in (4) runs as follows. From $(p) = \mathfrak{p}\mathfrak{p}'$, $\mathfrak{p}$ must have norm p, which makes $\mathbf{Z}[\sqrt{-5}]/\mathfrak{p}$ a field of size $\mathrm{N}(\mathfrak{p}) = p$, and that makes the natural map $\mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}[\sqrt{-5}]/\mathfrak{p}$ an isomorphism of fields. Since -5 is a square in $\mathbf{Z}[\sqrt{-5}]/\mathfrak{p}$, it is also a square in $\mathbf{Z}/p\mathbf{Z}$, so $-5 \equiv \square \bmod p$.)

Next we show

$$p = x^2 + 5y^2 \text{ for some } x, y \in \mathbf{Z} \iff (p) = \mathfrak{p}\mathfrak{p}' \text{ with principal } \mathfrak{p}, \mathfrak{p}'. \tag{5}$$

The key point is that the prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$ in (5) are principal.

($\Rightarrow$) If $p = x^2 + 5y^2$ for some x and y in $\mathbf{Z}$, then $(p) = (x + y\sqrt{-5})(x - y\sqrt{-5})$. The principal ideals on the right both have norm $x^2 + 5y^2 = p$, so they are prime ideals.

($\Leftarrow$) Suppose $(p) = (\alpha)(\beta)$ where (α) and (β) are principal prime ideals. Taking norms of both sides shows (α) and (β) have norm p. Writing $\alpha = x + y\sqrt{-5}$, we get $p = \mathrm{N}((\alpha)) = |x^2 + 5y^2| = x^2 + 5y^2$.

Finally, we show

$$2p = x^2 + 5y^2 \text{ for some } x, y \in \mathbf{Z} \iff (p) = \mathfrak{p}\mathfrak{p}' \text{ with nonprincipal } \mathfrak{p}, \mathfrak{p}'. \tag{6}$$

($\Rightarrow$) If $2p = x^2 + 5y^2$ for some integers x and y, then $(x + y\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}$, where $\mathfrak{p}$ has norm p. The ideal $\mathfrak{p}$ can't be principal, because if it were then $\mathfrak{p}_2$ would be a principal fractional ideal and thus a principal ideal, but we know $\mathfrak{p}_2$ is not a principal ideal. Similarly, $(x - y\sqrt{-5})$ has ideal norm $2p$ so $(x - y\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}'$, where $\mathfrak{p}'$ has norm p and $\mathfrak{p}'$ is not principal. Multiplying these factorizations of $(x + y\sqrt{-5})$ and $(x - y\sqrt{-5})$, we get

$$(2p) = (x + y\sqrt{-5})(x - y\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}\mathfrak{p}_2\mathfrak{p}' = \mathfrak{p}_2^2\mathfrak{p}\mathfrak{p}' = (2)\mathfrak{p}\mathfrak{p}',$$

so $(p) = \mathfrak{p}\mathfrak{p}'$ with nonprincipal $\mathfrak{p}$ and $\mathfrak{p}'$.

($\Leftarrow$) If $(p) = \mathfrak{p}\mathfrak{p}'$ with nonprincipal prime factors, then $\mathfrak{p}$ and $\mathfrak{p}'$ have norm p. Because there are only two ideal classes, the product of two nonprincipal ideals is principal, so $\mathfrak{p}_2\mathfrak{p} = (x+y\sqrt{-5})$ for some x and y in $\mathbf{Z}$. Taking the norm of both sides, $2p = |x^2+5y^2| = x^2+5y^2$.

Since the right sides of (5) and (6) are not compatible, by unique factorization of ideals, (4) tells us that $-5 \equiv \square \bmod p$ is equivalent to p or $2p$ being a value of $x^2 + 5y^2$ but both can't happen. □

The condition $2p = x^2 + 5y^2$ can be recast in terms of a representation theorem for p itself: $p = 2m^2 + 2mn + 3n^2$ for some $m, n \in \mathbf{Z}$. If $2p = x^2 + 5y^2$ then reducing mod 2 gives $0 \equiv x^2 + y^2 \equiv x + y \bmod 2$, so $x \equiv y \bmod 2$. Write $x = y + 2m$, so

$$2p = (y + 2m)^2 + 5y^2 = 4m^2 + 4my + 6y^2 \Longrightarrow p = 2m^2 + 2my + 3y^2.$$

Conversely, if $p = 2m^2 + 2mn + 3n^2$, then $2p = 4m^2 + 4mn + 6n^2 = (2m + n)^2 + 5n^2$. Therefore Theorem 3.2 can be recast as saying

$$-5 \equiv \square \bmod p \iff p \text{ is } x^2 + 5y^2 \text{ or } 2x^2 + 2xy + 3y^2 \text{ for some } x, y \in \mathbf{Z}, \tag{7}$$

and only one of these possibilities occurs.

Equation (7) is the way Gauss and Lagrange would have said $\mathbf{Q}(\sqrt{-5})$ has 2 ideal classes.

Here is another application of knowledge of the ideal class group of $\mathbf{Q}(\sqrt{-5})$.

Theorem 3.3. *The equation $y^2 = x^3 - 5$ has no integral solutions.*

This theorem can be proved by elementary methods with congruences, making no use of algebraic number theory, so the proof of this theorem below should be regarded just as an illustration of techniques.

Proof. Assuming $y^2 = x^3 - 5$ for integers x and y, we start with a parity check. If x is even then $y^2 \equiv -5 \equiv 3 \bmod 8$, but 3 mod 8 is not a square. Therefore x is odd, so y is even.

Write the equation as

$$x^3 = y^2 + 5 = (y + \sqrt{-5})(y - \sqrt{-5}). \tag{8}$$

Suppose δ is a common factor of $y+\sqrt{-5}$ and $y-\sqrt{-5}$ in $\mathbf{Z}[\sqrt{-5}]$. First of all, $\mathrm{N}(\delta)$ divides $y^2 + 5$, which is odd. Second of all, since δ divides $(y + \sqrt{-5}) - (y - \sqrt{-5}) = 2\sqrt{-5}$, $\mathrm{N}(\delta)$ divides $\mathrm{N}(2\sqrt{-5}) = 20$. Therefore $\mathrm{N}(\delta)$ is 1 or 5. If $\mathrm{N}(\delta) = 5$ then $5|(y^2 + 5)$, so $5|y$. Then $x^3 = y^2+5 \equiv 0 \bmod 5$, so $x \equiv 0 \bmod 5$. Now x and y are both multiples of 5, so $5 = x^3 - y^2$ is a multiple of 25, a contradiction. Hence $\mathrm{N}(\delta) = 1$, so δ is a unit. This shows $y + \sqrt{-5}$ and $y - \sqrt{-5}$ have no common factor in $\mathbf{Z}[\sqrt{-5}]$ except for units.

Since $y + \sqrt{-5}$ and $y - \sqrt{-5}$ are relatively prime elements and their product is a cube, if $\mathbf{Z}[\sqrt{-5}]$ were a UFD then they would both be cubes (the units in $\mathbf{Z}[\sqrt{-5}]$ are ± 1, which

are both cubes). Since $\mathbf{Z}[\sqrt{-5}]$ is not a UFD that reasoning is incorrect, but the conclusion is nevertheless correct: if x and y are integers satisfying (8) then $y \pm \sqrt{-5}$ are cubes. To see why, pass from (8) as an equation of elements to an equation of principal ideals:

$$(x)^3 = (y + \sqrt{-5})(y - \sqrt{-5}).$$

We will show the ideals $(y + \sqrt{-5})$ and $(y - \sqrt{-5})$ are relatively prime and then appeal to unique factorization of ideals. (The relative primality of the ideals is not an automatic consequence of the relative primality of the generators as elements of $\mathbf{Z}[\sqrt{-5}]$. For example, $1+\sqrt{-5}$ and $1-\sqrt{-5}$ have no common factors in $\mathbf{Z}[\sqrt{-5}]$ besides ± 1, but the ideals $(1+\sqrt{-5})$ and $(1 - \sqrt{-5})$ have common factor $(1 + \sqrt{-5}, 1 - \sqrt{-5}) = (2, 1 + \sqrt{-5})$, a (nonprincipal) prime ideal.)

If $(y + \sqrt{-5})$ and $(y - \sqrt{-5})$ are not relatively prime ideals then they are both divisible by some prime ideal $\mathfrak{p}$. Then

$$y + \sqrt{-5} \equiv 0 \bmod \mathfrak{p}, \quad y - \sqrt{-5} \equiv 0 \bmod \mathfrak{p},$$

so subtracting gives $2\sqrt{-5} \equiv 0 \bmod \mathfrak{p}$. Thus $(2\sqrt{-5}) \subset \mathfrak{p}$, so $\mathfrak{p} \mid (2\sqrt{-5})$. Taking norms, $\mathrm{N}(\mathfrak{p})$ divides $\mathrm{N}((2\sqrt{-5})) = 20$. Also $\mathrm{N}(\mathfrak{p})$ divides $\mathrm{N}((y + \sqrt{-5})) = y^2 + 5$, which is odd, so $\mathrm{N}(\mathfrak{p}) = 5$. Thus 5 divides $y^2 + 5$, so $5 \mid y$. Then $x^3 = y^2 + 5 \equiv 5 \bmod 25$, which has no solution. So the ideals $(y + \sqrt{-5})$ and $(y - \sqrt{-5})$ are relatively prime.

Since the ideals $(y + \sqrt{-5})$ and $(y - \sqrt{-5})$ multiply to the cube of an ideal and are relatively prime, they are each cubes of ideals:

$$(y + \sqrt{-5}) = \mathfrak{a}^3, \quad (y - \sqrt{-5}) = \mathfrak{b}^3.$$

Passing to the ideal class group, $[\mathfrak{a}]^3$ is trivial, so $[\mathfrak{a}]$ has order dividing 3. Since the class group of $\mathbf{Z}[\sqrt{-5}]$ has order 2, $[\mathfrak{a}]$ has order 1, which means $\mathfrak{a}$ is principal, say $\mathfrak{a} = (\alpha)$. Therefore $(y+\sqrt{-5}) = (\alpha)^3 = (\alpha^3)$, so $y+\sqrt{-5} = u\alpha^3$, where $u \in \mathbf{Z}[\sqrt{-5}]^\times = \{\pm 1\}$. Since ± 1 are both cubes, we can absorb them into α and thus write

$$y + \sqrt{-5} = (m + n\sqrt{-5})^3 \tag{9}$$

for some integers m and n. Expanding the cube and equating real and imaginary parts on both sides,

$$y = m^3 - 15mn^2 = m(m^2 - 15n^2), \quad 1 = 3m^2n - 5n^3 = n(3m^2 - 5n^2).$$

From the second equation, $n = \pm 1$. If $n = 1$ then $1 = 3m^2 - 5$, so $3m^2 = 6$, which has no integral solution. If $n = -1$ then $1 = -(3m^2 - 5)$, so $3m^2 = 4$, which also has no integral solution. Thus $y^2 = x^3 - 5$ has no integral solutions. □

The key point in this approach to $y^2 = x^3 - 5$ is not so much that the ideal class group of $\mathbf{Q}(\sqrt{-5})$ has order 2 but rather that its order is relatively prime to 3, so $\mathfrak{a}^3$ being principal makes $\mathfrak{a}$ principal. More generally, finding the integral solutions to $y^2 = x^3 + k$ when the order of the ideal class group of $\mathbf{Q}(\sqrt{k})$ is relatively prime to 3 proceeds "as if" the ideal class group were trivial.

Ideal class groups are used to study integral solutions of $y^2 = x^3 + k$ not only quantitatively for specific k but also qualitatively for general k. For any integer $k \neq 0$, the equation $y^2 = x^3 + k$ has only finitely many integral solutions (x, y) and this is proved using finiteness of ideal class groups, although in a different way than we used them for $k = -5$. See [18, Chap. IX] for the proof, which also involves techniques from Diophantine approximations and algebraic geometry.

4. More Examples

For a number field K, here is a procedure for finding $\mathrm{Cl}(K)$:

- Pick a $\mathbf{Z}$-basis for $\mathcal{O}_K$, say $\{e_1, \ldots, e_n\}$.
- Set the Kronecker bound to be
$$C = \prod_{\sigma\colon K \to \mathbf{C}} \Big(\sum_{i=1}^{n} |\sigma(e_i)|\Big).$$
The group $\mathrm{Cl}(K)$ is generated by primes $\mathfrak{p}$ where $\mathrm{N}(\mathfrak{p}) \leqslant C$.
- Find all primes $\mathfrak{p}$ such that $\mathrm{N}(\mathfrak{p}) \leqslant C$.
- Figure out relations among $[\mathfrak{p}]$ where $\mathrm{N}(\mathfrak{p}) \leqslant C$.

Writing $\mathrm{N}(\mathfrak{p}) = p^f$, if $\mathrm{N}(\mathfrak{p}) \leqslant C$ then $p \leqslant C$, so we factor all (p) where $p \leqslant C$ and look at its prime ideal factors with norm at most C to get generators for $\mathrm{Cl}(K)$. The last step above is the hardest. You may happen to find enough elements in $\mathcal{O}_K$ to show all the prime ideals in your list are principal (*e.g.*, if $\alpha \in \mathfrak{p}$ and $\big|\mathrm{N}_{K/\mathbf{Q}}(\alpha)\big| = \mathrm{N}(\mathfrak{p})$, then $\mathfrak{p} = (\alpha)$), in which case $h = 1$, but if you are left with some ideals that you suspect are not principal and want to prove they aren't (so $h > 1$), how do you do that? One way to show $\mathfrak{a}$ is not principal is to compute $\mathrm{N}(\mathfrak{a})$ and, after crossing your fingers, hope you can show there is no element α such that $\big|\mathrm{N}_{K/\mathbf{Q}}(\alpha)\big| = \mathrm{N}(\mathfrak{a})$.

Example 4.1. Let $K = \mathbf{Q}(\sqrt{13})$ and $\mathcal{O}_K = \mathbf{Z}[\frac{1+\sqrt{13}}{2}]$. Using $\{1, \frac{1+\sqrt{13}}{2}\}$ as a $\mathbf{Z}$-basis for $\mathcal{O}_K$,
$$C = \left(1 + \left|\frac{1+\sqrt{13}}{2}\right|\right)\left(1 + \left|\frac{\sqrt{13}-1}{2}\right|\right) = 4 + \sqrt{13} \approx 7.6.$$
We need to factor all (p) where $p \leqslant 7$. That means we will factor $T^2 - T - 3 \bmod p$ for $p = 2$, 3, 5, and 7. See Table 1 below. The prime ideals with norm at most 7 are (2), $\mathfrak{p}_3$,

p	$T^2 - T - 3 \bmod p$	(p)
2	irreducible	(2)
3	$T(T-1)$	$\mathfrak{p}_3\mathfrak{p}_3'$
5	irreducible	(5)
7	irreducible	(7)

Table 1. Factoring prime numbers in $\mathbf{Z}[\frac{1+\sqrt{13}}{2}]$.

and $\mathfrak{p}_3'$. (The ideal (5) has norm 25 and the ideal (7) has norm 49.) Since $\mathrm{N}(4 \pm \sqrt{13}) = 3$, and $4 + \sqrt{13}$ and $4 - \sqrt{13}$ are not unit multiples in $\mathcal{O}_K$, the ideals $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ are $(4 \pm \sqrt{13})$, so they are principal. Therefore every prime ideal with norm at most 7 is principal, which implies $\mathrm{Cl}(\mathcal{O}_K)$ is trivial. Thus $\mathbf{Z}[\frac{1+\sqrt{13}}{2}]$ is a PID, and we did not show this by checking if the ring is Euclidean. (It is Euclidean, but we don't discuss how to show that.)

Example 4.2. Let $K = \mathbf{Q}(\sqrt{-23})$ and as a $\mathbf{Z}$-basis of $\mathcal{O}_K$ choose $\{1, \frac{1+\sqrt{-23}}{2}\}$, which implies
$$C = \left(1 + \left|\frac{1+\sqrt{-23}}{2}\right|\right)\left(1 + \left|\frac{1-\sqrt{-23}}{2}\right|\right) \approx 11.8.$$
Table 2 lists the factorization of $T^2 - T + 6 \bmod p$ for $p \leqslant C$.

p	$T^2 - T + 6 \bmod p$	(p)
2	$T(T-1)$	$\mathfrak{p}_2\mathfrak{p}_2'$
3	$T(T-1)$	$\mathfrak{p}_3\mathfrak{p}_3'$
5	irreducible	(5)
7	irreducible	(7)
11	irreducible	(11)

TABLE 2. Factoring prime numbers in $\mathbf{Z}[\frac{1+\sqrt{-23}}{2}]$.

The primes ideals with norm at most 11 in $\mathbf{Q}(\sqrt{-23})$ are $\mathfrak{p}_2, \mathfrak{p}_2', \mathfrak{p}_3$, and $\mathfrak{p}_3'$. Since $\mathfrak{p}_2\mathfrak{p}_2' = (2)$ and $\mathfrak{p}_3\mathfrak{p}_3' = (3)$, in $\mathrm{Cl}(K)$ we have the relations $[\mathfrak{p}_2'] = [\mathfrak{p}_2]^{-1}$ and $[\mathfrak{p}_3'] = [\mathfrak{p}_3]^{-1}$. Since $\mathrm{N}((\frac{1+\sqrt{-23}}{2})) = 6$, we can set $(\frac{1+\sqrt{-23}}{2}) = \mathfrak{p}_2\mathfrak{p}_3$. (This equation distinguishes $\mathfrak{p}_2$ from $\mathfrak{p}_2'$ and $\mathfrak{p}_3$ from $\mathfrak{p}_3'$, which up to this point have appeared in symmetric roles.) So $[\mathfrak{p}_3] = [\mathfrak{p}_2]^{-1}$. Thus $\mathrm{Cl}(K) = \langle[\mathfrak{p}_2]\rangle$. Is $\mathfrak{p}_2$ principal? This ideal has norm 2, and for $m, n \in \mathbf{Z}$,

$$\mathrm{N}\left(m + n\frac{1+\sqrt{-23}}{2}\right) = \left(m + \frac{n}{2}\right)^2 + 23\left(\frac{n}{2}\right)^2,$$

which is never 2. (For nonzero n the norm is at least $23/4 > 2$ and for $n = 0$ the norm is a perfect square.) Since no $\alpha \in \mathcal{O}_K$ has norm 2, $[\mathfrak{p}_2] \neq 1$. Also

$$\mathrm{N}\left(1 + \frac{1+\sqrt{-23}}{2}\right) = \mathrm{N}\left(\frac{3}{2} + \frac{1}{2}\sqrt{-23}\right) = 8.$$

Since

$$\frac{1+\sqrt{-23}}{2} \equiv 0 \bmod \mathfrak{p}_2 \Longrightarrow 1 + \frac{1+\sqrt{-23}}{2} \equiv 1 \not\equiv 0 \bmod \mathfrak{p}_2,$$

we must have $(1 + \frac{1+\sqrt{-23}}{2}) = \mathfrak{p}_2'^3$, so $[\mathfrak{p}_2']^3 = 1$ and therefore $[\mathfrak{p}_2]^3 = 1$. This shows $[\mathfrak{p}_2]$ has order 3, so $\mathrm{Cl}(K) = \{[(1)], [\mathfrak{p}_2], [\mathfrak{p}_2^2]\}$. For any nonzero ideal $\mathfrak{a}$ in $\mathbf{Z}[\frac{1+\sqrt{-23}}{2}]$,

- $\mathfrak{a}^3$ is principal since $[\mathfrak{a}]^3 = 1$,
- either $\mathfrak{a}$ is principal or $\mathfrak{a}\mathfrak{p}_2$ is principal (if $[\mathfrak{a}] = [\mathfrak{p}_2^2]$) or $\mathfrak{a}\mathfrak{p}_2^2$ is principal (if $[\mathfrak{a}] = [\mathfrak{p}_2]$) and only one of these can happen.

The next two examples show the Kronecker bound C can get big for fields of small degree.

Example 4.3. Let $K = \mathbf{Q}(\alpha)$ where $\alpha^3 - \alpha - 1 = 0$, so $\mathcal{O}_K = \mathbf{Z}[\alpha]$ (the discriminant is squarefree). Using the $\mathbf{Z}$-basis $\{1, \alpha, \alpha^2\}$, $C \approx 28.08$.

Example 4.4. Let $K = \mathbf{Q}(\beta)$ where $\beta^5 - \beta - 1 = 0$, so $\mathcal{O}_K = \mathbf{Z}[\beta]$ (the discriminant is squarefree). Using the $\mathbf{Z}$-basis $\{1, \beta, \beta^2, \beta^3, \beta^4\}$, $C \approx 3454.4$.

By changing the $\mathbf{Z}$-basis we can get some savings in C.

Example 4.5. In $\mathbf{Z}[\sqrt{103}]$ with $\mathbf{Z}$-basis $\{1, \sqrt{103}\}$, $C \approx 124.29$. Replacing $\sqrt{103} \approx 10.14$ with the smaller number $\sqrt{103} - 10$ gives us a $\mathbf{Z}$-basis $\{1, \sqrt{103} - 10\}$ for which $C \approx 24.29$.

In Table 3 we list the first squarefree positive and negative d for which the quadratic field $\mathbf{Q}(\sqrt{d})$ has each possible class group structure from sizes 2 to 9. For example, the first imaginary quadratic field $\mathbf{Q}(\sqrt{d})$, ordered by $|d|$, whose class group is a product of two groups of order 2 occurs when $d = -21$.

Group	$\mathbf{Z}/2\mathbf{Z}$	$\mathbf{Z}/3\mathbf{Z}$	$\mathbf{Z}/4\mathbf{Z}$	$(\mathbf{Z}/2\mathbf{Z})^2$	$\mathbf{Z}/5\mathbf{Z}$	$\mathbf{Z}/6\mathbf{Z}$
$d > 0$	10	79	82	130	401	235
$d < 0$	-5	-23	-14	-21	-47	-26
Group	$\mathbf{Z}/7\mathbf{Z}$	$\mathbf{Z}/8\mathbf{Z}$	$\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$	$(\mathbf{Z}/2\mathbf{Z})^3$	$\mathbf{Z}/9\mathbf{Z}$	$(\mathbf{Z}/3\mathbf{Z})^2$
$d > 0$	577	226	399	1155	1129	32009
$d < 0$	-71	-41	-65	-105	-199	-4027

TABLE 3. Quadratic fields $\mathbf{Q}(\sqrt{d})$ with particular class groups.

5. The Class Number

The number of ideal classes in a number field K (really, the number of ideal classes in $\mathcal{O}_K$) is called the *class number* of K and is written $h(K)$.[1] Saying $h(K) = 1$ is another way of saying $\mathcal{O}_K$ is a PID. We know that $h(\mathbf{Q}) = 1$, $h(\mathbf{Q}(i)) = 1$, $h(\mathbf{Q}(\sqrt{-5})) = 2$, and $h(\mathbf{Q}(\sqrt{-23})) = 3$.

The importance of class numbers in Diophantine equations is illustrated by Kummer's work on Fermat's last theorem., which was Fermat's claim that he could show, by a marvelous proof that didn't fit in the margin, that the equation $x^n + y^n = z^n$ has no solution in positive integers x, y, and z when $n \geqslant 3$. If this is true for an exponent n then it is true for any multiple of n. Every number $n \geqslant 3$ is divisible by an odd prime or by 4, so it suffices to focus on these exponents. Fermat himself had settled the case $n = 4$, so suppose $x^p + y^p = z^p$ where p is an odd prime and x, y, and z are positive integers. Any common factor of x or y is a factor of z and the p-th power of this factor can be cancelled from all the terms, so we may assume $(x, y) = 1$. The sum $x^p + y^p$ can be factored using pth roots of unity as $\prod_{i=0}^{p-1}(x + \zeta_p^i y)$, where ζ_p is a nontrivial pth root of unity, so the Fermat equation $x^p + y^p = z^p$ can be rewritten as

$$\prod_{i=0}^{p-1}(x + \zeta_p^i y) = z^p. \tag{10}$$

This equation is in $\mathbf{Z}[\zeta_p]$, which is the ring of integers of $\mathbf{Q}(\zeta_p)$, although Kummer did not know this; for him $\mathbf{Z}[\zeta_p]$ was just the natural ring to work in for this problem.

If $\mathbf{Z}[\zeta_p]$ has unique factorization and the factors on the left side of (10) are pairwise relatively prime, then each factor is a pth power up to unit multiple: $x + \zeta_p^i y = u_i w_i^p$. For $x + \zeta_p^i y$ to be nearly a pth power for all i from 0 to $p-1$ seems like a very strong condition to impose on two integers x and y, so one can anticipate that there should be a contradiction from this. Kummer devised a method to make this intuition precise, but he knew that it was not automatic for the factors $x + \zeta_p^i y$ to be relatively prime and he also discovered that the assumption of unique factorization is wrong when $p = 23$. He found a class number hypothesis that allowed him to get around these problems.

Theorem 5.1 (Kummer, 1847)**.** *If p is an odd prime and $p \nmid h(\mathbf{Q}(\zeta_p))$ then $x^p + y^p = z^p$ has no solution in positive integers x, y, z.*

The importance of p not dividing $h(\mathbf{Q}(\zeta_p))$ for Kummer was similar to the importance of 3 not dividing $h(\mathbf{Q}(\sqrt{-5}))$ in the proof of Theorem 3.3: if $p \nmid h(\mathbf{Q}(\zeta_p))$ then an ideal in $\mathbf{Z}[\zeta_p]$ whose pth power is principal has to be principal: if $\mathfrak{a}^p = (\alpha)$ then $[\mathfrak{a}]^p = 1$, so $[\mathfrak{a}] = 1$

[1]The use of h as the notation for the number of ideal classes goes back to Dirichlet (1838).

when $[\mathfrak{a}]$ doesn't have order p. This is useful if we want to convert (10) into an equation with ideals and later come back to recover information about numbers. A proof of Theorem 5.1 is in [3, pp. 223–224, 378–381]. It is not easy and requires subtle properties of units in $\mathbf{Z}[\zeta_p]$. For comparison, $\mathbf{Z}[\sqrt{-5}]$ has units ± 1 so there are no unit problems in Theorem 3.3.

For prime p it turns out that $h(\mathbf{Q}(\zeta_p)) = 1$ for $p \leqslant 19$, and Table 4 lists $h(\mathbf{Q}(\zeta_p))$ for all the remaining primes p below 50. We see 37 is the only prime in this range that does not fit the hypothesis in Kummer's theorem, so Kummer had proved Fermat's last theorem for every prime exponent below 50 other than $p = 37$, which was a striking achievement compared to other work on Fermat's last theorem at the time. Before Kummer, the only settled cases of Fermat's Last Theorem for prime exponent p were $p = 3, 5$, and 7. (Kummer did *not* actually compute all the class numbers in Table 4. He found a method to decide if $p \nmid h(\mathbf{Q}(\zeta_p))$ that is simpler to carry out by hand than computing $h(\mathbf{Q}(\zeta_p))$.)

p	23	29	31	37	41	43	47
$h(\mathbf{Q}(\zeta_p))$	3	2^3	3^2	37	11^2	211	$5 \cdot 139$

TABLE 4. Class number of $\mathbf{Q}(\zeta_p)$.

The class numbers in Table 4 are growing, and Kummer conjectured that $h(\mathbf{Q}(\zeta_p)) = 1$ only for $p \leqslant 19$. This was proved independently by Montgomery and Uchida in 1971. Ultimately Fermat's last theorem was settled completely by Wiles and Taylor [20], [21] using techniques that make no use whatsoever of factorizations like (10).

There are many open questions about ideal class groups of number fields. Here are a few of them, which are all believed to have the answer "yes."

(1) Are there infinitely many number fields with class number 1? It has been suggested that the number fields $\mathbf{Q}(\zeta_{2^n} + \zeta_{2^n}^{-1}) = \mathbf{Q}(\cos(2\pi/2^n))$ all have class number 1. Weber showed 2 is not a factor of any class number in this list. Fukuda and Komatsu [9] showed a prime factor of any class number in this list is greater than 10^9.

(2) Are there infinitely many real quadratic fields with class number 1? This goes back to Gauss. The data suggest that for about 76% of prime numbers p, the field $\mathbf{Q}(\sqrt{p})$ has class number 1. In contrast to real quadratic fields, it is known by work of Baker [1], Heegner [11], and Stark [19] that there are only 9 imaginary quadratic fields with class number 1: $\mathbf{Q}(\sqrt{d})$ for $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$. The strikingly different behavior of class numbers of real and imaginary quadratic fields is related to the unit group being infinite in the real quadratic case and finite in the imaginary quadratic case. It's usually hard to separate the study of ideal class groups and unit groups (*e.g.*, to prove an ideal is nonprincipal we usually need to know about the units), but in the imaginary quadratic case the unit group is finite and explicitly known.

(3) Are there infinitely many quadratic fields where the subgroup of ideal classes of odd order in the class group, called the odd part of the class group, is cyclic? (The 2-Sylow subgroup of the class group of a quadratic field is generally not cyclic.) In examples, the odd part of the class group shows a definite bias for being cyclic. Notice, for instance, how much larger $|d|$ is in Table 3 when $\mathbf{Q}(\sqrt{d})$ first has a noncyclic class group of size 9 compared to the first cyclic class group of size 9. The Cohen–Lenstra heuristics [7] give precise conjectures about the frequency with which the odd part of the class group of a quadratic field has specific structural properties

(*e.g.*, being cyclic, having order divisible by a particular prime, having a particular p-Sylow subgroup). Their heuristics were extended to class groups of higher-degree number fields by Cohen and Martinet [8]. Numerical data once cast some doubt on the higher-degree heuristics, but a special case of the Cohen–Martinet heuristics was proved by Bhargava [2].

(4) Does each finite abelian group arise (up to isomorphism) as the class group of some number field? Table 3 might suggest that every finite abelian group could be the class group of a real and imaginary quadratic field, but this is not true: Chowla [15, p. 447] showed $(\mathbf{Z}/2\mathbf{Z})^n$ is not the class group of any imaginary quadratic field for all large n (probably $n \geqslant 5$ is enough; all $n < 5$ occur) and Shanks [17] showed no imaginary quadratic field has class group $(\mathbf{Z}/5\mathbf{Z})^2$, $(\mathbf{Z}/7\mathbf{Z})^2$, or $(\mathbf{Z}/11\mathbf{Z})^2$. The real quadratic case is different, *e.g.*, the Cohen–Lenstra heuristics predict that each finite abelian group of odd order should be the odd part of the class group of infinitely many real quadratic fields.

(5) Are there infinitely many regular primes? A prime number p is called *regular* if $p \nmid h(\mathbf{Q}(\zeta_p))$. These are the primes to which Kummer's work on Fermat's last theorem can be applied. Below 100 all primes are regular except for 37, 59, and 67. (The fields $\mathbf{Q}(\zeta_{37})$, $\mathbf{Q}(\zeta_{59})$, and $\mathbf{Q}(\zeta_{67})$ have class numbers 37, $3 \cdot 59 \cdot 233$, and $67 \cdot 12739$, respectively.) It is known that there are infinitely many irregular primes [3, pp. 381–382], and all the numerical data suggest regular primes appear more often than irregular primes, but there is no proof that there actually are infinitely many regular primes.

(6) For each prime p, is the class number of the maximal real subfield $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$ of $\mathbf{Q}(\zeta_p)$ not divisible by p? This is Vandiver's conjecture. It has been checked into the millions, although probabilistic heuristics suggest counterexamples would occur only rarely, so the lack of counterexamples so far is not yet compelling.

The behavior of class numbers in towers of number fields is not straightforward. For cyclotomic fields, there is divisibility in towers: if $\mathbf{Q}(\zeta_m) \subset \mathbf{Q}(\zeta_n)$ then $h(\mathbf{Q}(\zeta_m)) \mid h(\mathbf{Q}(\zeta_n))$. But in general if $K \subset L$ it need not be true that $h(K) \mid h(L)$, or even that $h(K) \leqslant h(L)$. For instance, $h(\mathbf{Q}(\sqrt{-5})) = 2$ but $h(\mathbf{Q}(i, \sqrt{-5})) = 1$.

It was believed for many years that every number field is a subfield of a number field with class number 1, but in 1964 Golod and Shafarevich [10] gave explicit counterexamples among imaginary quadratic fields. Brumer [4], Kuzmin [14], and Roquette and Zassenhaus [16] extended this work and it turns out that there are infinitely many counterexamples in each degree greater than 1.

References

[1] A. Baker, Linear forms in the logarithms of algebraic numbers I, *Mathematika* **13** (1966), 204–216

[2] M. Bhargava, The density of discriminants of quartic rings and fields, *Ann. of Math.* **162** (2005), 1031–1063.

[3] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, 1966.

[4] A. Brumer, Ramification and class towers of number fields, *Michigan J. Math.* **12** (1965), 129–131.

[5] L. Claborn, Every abelian group is a class group, *Pacific J. Math.* **18** (1966), 219–222.

[6] P. L. Clark, Elliptic Dedekind domains revisited, *Enseign. Math.* **55** (2009), 213–225.

[7] H. Cohen and H. W. Lenstra, Heuristics on class groups of number fields, *Lecture Notes in Mathematics* **1068**, 33–62, 1984.

[8] H. Cohen and J. Martinet, Étude heuristique des groupes de classes des corps de nombres, *J. Reine Angew. Math.* **404** (1980), 39–76.

[9] T. Fukuda and K. Komatsu, Weber's class number problem in the cyclotomic $\mathbf{Z}_2$-extension of $\mathbf{Q}$, III, *Int. J. Number Theory* **7** (2009), 1627–1635.
[10] E. S. Golod and I. R. Shafarevich, On the class-field tower, *Izv. Akad. Nauk SSSR, Ser. Mat. (Russian)* **29** (1964), 261–272.
[11] K. Heegner, Diophantintische Analysis und Modulfunktionen, *Math. Z.* **56** (1952), 227–253.
[12] L. Kronecker, Grundzüge einer arithmetischen Theorie der algebraischen Grössen, *J. Reine Angew. Math.* **92** (1882), 1–122.
[13] L. Kronecker, De unitatibus complexis, *J. Reine Angew. Math.* **93** (1882), 1–52.
[14] L. V. Kuzmin, Homologies of profinite groups, the schur multiplier and class field theory, *Izv. Akad. Nauk SSSR, Ser. Mat. (Russian)* **33** (1969), 1220–1254.
[15] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer-Verlag, 3rd edition, 2004.
[16] P. Roquette and H. Zassenhaus, A class rank estimate for algebraic number fields, *J. London Math. Soc.* **44** (1969), 31–38.
[17] D. Shanks, On Gauss's class number problems, *Math. Comp.* **23** (1969), 151–163.
[18] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.
[19] H. M. Stark, A complete determination of the complex quadratic fields of class-number one, *Michigan Math. J.* **14** (1967), 1–27.
[20] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. of Math.* **141** (1995), 553–572.
[21] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* **141** (1995), 443–551.