CUBIC RESIDUACITY AND QUADRATIC FORMS

FRANZ LEMMERMEYER

Dedicated to the memory of Harvey Cohn (1923–2014)

Abstract. In 1900, Dedekind published his article [7] on the class number of pure cubic number fields. Here we will explain parts of Dedekind’s results.

The claim that Dedekind’s article [7] contains the proof that for pure cubic number fields \( K \), the quotient of zeta functions \( \zeta_K(s)/\zeta(s) \) is entire (extends to a holomorphic function on the whole complex plane) is all over the place in the modern literature, and probably goes back to a statement made by Artin in 1923. The conjecture that for extensions \( K/k \) of number fields, the quotient \( \zeta_K(s)/\zeta_k(s) \) is an entire function was named after Dedekind by Robert van der Waall in 1974. Dedekind, however, had nothing at all to do with this conjecture, and apparently it was Landau [16, p. 390] who first asked whether this result is true:

\[ I \text{have to be careful with its formulation since it is not known whether } \frac{\zeta_k(s)}{\zeta(s)} \text{ is always an entire function.} \]

At the time when Dedekind wrote his article, the Dedekind zeta function was not yet extended to the whole complex plane (this was first done by Hecke). Dedekind did show that for pure cubic number fields \( K \), the quotient \( \zeta_K(s)/\zeta(s) \) may be expressed as a linear combination of zeta functions now named after Epstein, who proved in 1903 that these are indeed entire functions.

The real content of Dedekind’s article. The central problem that Dedekind is dealing with in [7] is the following: How can we prove that 2 is a cubic residue of a prime number \( p \equiv 1 \mod 3 \) if and only if \( p \) is represented by the quadratic form \( x^2 + 27y^2 \)? The methods that Gauß presented in his Disquisitiones Arithmeticae are sufficient for proving this claim, and the proof becomes a simple exercise using the cubic reciprocity law proved by Jacobi and Eisenstein. But these proofs do not explain the intimate connection between the quadratic form \( x^2 + 27y^2 \) and the cubic residuacity of 2: The form \( x^2 + 27y^2 \) is the norm form of the order \( \mathbb{Z} \oplus \mathbb{Z}[3\sqrt{-3}] \) in the quadratic number field \( \mathbb{Q}(\sqrt{-3}) \), the latter is just a reflection of the decomposition law of prime ideals in the pure cubic number field \( \mathbb{Q}(\sqrt[3]{2}) \).

Dedekind’s efforts of finding a conceptual proof of this simple number theoretic statement led him to the construction of a connection between ring class groups in quadratic number fields on the one hand and pure cubic number fields on the other hand. This clearly implies that Dedekind’s work on cubic residuacity in [7] can only be properly understood within the framework of class field theory, which was developed almost half a century after Dedekind had started his investigation in the 1870s.

It is well known that the quadratic reciprocity law is closely related to the theory of binary quadratic forms. Cox’s beautiful book [6] and the recent work by Bhargava [1, 2] on Gauß composition have done much to promote the theory of binary quadratic forms. The present article, whose main aim is the resurrection of a rarely read memoir by Richard Dedekind,
should be seen as an effort to support their agenda of reviving the theory of binary quadratic forms.

1. Euler

In Euler’s time, number theory was often looked down upon as some form of recreational mathematics. It is therefore rather remarkable that Euler started writing a textbook on number theory (for a nonexistent market), which unfortunately was never completed, and the draft of Euler’s book was published only in 1849. The most interesting part of his Tractatus, as his manuscript [8] is usually called, is concerned with the theory of cubic and quartic residues. As Fermat in his early number theoretical investigations, Euler looked at factors of numbers of the form $2^n - 1$.

Primes $n$ that divide $2^{n+1} - 1$ are, by Euler’s criterion, those for which 2 is a quadratic residue. Euler now studied primes $n \equiv 1 \mod 3$ that divide $2^{n+1} - 1$ and remarked that a prime number $n$ divides $2^{n+1} - 1$ if and only if 2 is a cubic residue modulo $n$. Among the primes $n \leq 100$, only $n = 31$ and $n = 43$ have this property.

Extending the table reveals that the pattern does not seem to involve the residue classes of $n$. Euler knows, however, that primes $n \equiv 1 \mod 3$ are represented by the quadratic form $p^2 + 3q^2$. Thus he writes the primes $n \leq 1093$ that divide $2^{n+1} - 1$ in the form $q^2 + 3p^2$:

<table>
<thead>
<tr>
<th>$n$</th>
<th>$p$</th>
<th>$q$</th>
<th>$n$</th>
<th>$p$</th>
<th>$q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>2</td>
<td>3</td>
<td>283</td>
<td>16</td>
<td>3</td>
</tr>
<tr>
<td>43</td>
<td>4</td>
<td>3</td>
<td>307</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>109</td>
<td>1</td>
<td>6</td>
<td>397</td>
<td>17</td>
<td>6</td>
</tr>
<tr>
<td>127</td>
<td>10</td>
<td>3</td>
<td>433</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>157</td>
<td>7</td>
<td>6</td>
<td>499</td>
<td>16</td>
<td>9</td>
</tr>
<tr>
<td>223</td>
<td>14</td>
<td>3</td>
<td>601</td>
<td>13</td>
<td>6</td>
</tr>
<tr>
<td>229</td>
<td>11</td>
<td>6</td>
<td>601</td>
<td>13</td>
<td>12</td>
</tr>
<tr>
<td>277</td>
<td>13</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

By carefully investigating the prime divisors of numbers of the form $2^n - 1$ he is led to a conjecture concerning the divisors of $2^{n+1} - 1$ for numbers $n \equiv 1 \mod 6$:

*If we ponder this matter very carefully then we observe that they all can be represented in the form $27pp + qq$ whenever it is a prime; but we cannot yet confirm this observation by a proof.*

Euler’s conjecture asserts that 2 is a cubic residue modulo $n$ if and only if $n = 27p^2 + q^2$. He then manages to provide similar criteria for the cubic residuacity of $a = 3, 5, 6, 7,$ and 10; we will be content with stating his conjectures for $a \leq 6$:

a) 2 is cubic residue modulo primes $p = 6n + 1 = q^2 + 3p^2$ if and only if $p$ is divisible by 3.

b) 3 is cubic residue modulo primes $p = 6n + 1 = q^2 + 3p^2$ if and only if $p$ or $p \pm q$ is divisible by 9.

c) 5 is cubic residue modulo primes $p = 6n + 1 = q^2 + 3p^2$ if and only if one of the following conditions is satisfied:
   i) $p$ is divisible by 15;
   ii) $p$ is divisible by 3 and $q$ by 5;
   iii) $p \pm q$ is divisible by 15;
   iv) $p \pm 2q$ is divisible by 15.

d) 6 is cubic residue modulo primes $p = 6n + 1 = q^2 + 3p^2$ if and only if $p$ or $2p \pm q$ is divisible by 9.
Euler couldn’t prove any of these conjectures, nor was he able to find a pattern for general values of \( a \). Seeing the correct generalization of these conjectures requires, as we will see, a lot more than just a passing familiarity with binary quadratic forms.

**The Language of Forms.** Let us now rewrite Euler’s conjectures in a form that is better suited for seeing patterns. We will also use \( p \) to denote a prime number \( p \equiv 1 \mod 3 \), write \( (a/p)_3 = 1 \) if \( a \) is a cubic residue modulo \( p \), and denote the binary quadratic form \( Ax^2 + Bxy + Cy^2 \) by \( (A, B, C) \). We say that a prime \( p \) is represented by \( (A, B, C) \) if there exist integers \( x, y \) such that \( p = Ax^2 + Bxy + Cy^2 \).

Euler already had seen that \((2/p)_3 = 1\) for primes \( p = x^2 + 3y^2 \) if and only if \( p \) is represented by the form \((1, 0, 27)\). Observe that the form \((1, 0, 3)\) has discriminant \(-3 \cdot 2^2\), and that the discriminant of \((1, 0, 27)\) is \(-3 \cdot 6^2\). The primes \( p \) with \((2/p)_3 \neq 1\) necessarily have the form \( p = x^2 + 3y^2 \) with \( y \equiv \pm 1 \mod 3 \). Since \( x \) is not divisible by 3 this means that such \( p \) are represented by \( x^2 + 3y^2 \) with \( y = 3z \pm x \):

\[
x^2 + 3(3z \pm x)^2 = 4x^2 \pm 18xz + 27z^2.
\]

The forms \((4, \pm 18, 27)\) have the same discriminant as \((1, 0, 27)\), namely \( \Delta = -108 = -3 \cdot 6^2 \).

Rewriting Euler’s other conjectures shows that the primes \( p \) seem to satisfy \((a/p)_3 = 1\) if and only if they are represented by certain forms with discriminant \(-3 \cdot f^2\) for some integer \( f | 6a \). What Euler lacked was a general theory of binary quadratic forms.

2. Quadratic Reciprocity and Quadratic Forms

Almost from the beginning of mathematics, sums of two squares have played a prominent role in what we nowadays call number theory. The question of Pythagorean triples, i.e., integral solutions of the Pythagorean equation \( x^2 + y^2 = z^2 \), was studied in all ancient cultures whose contributions have survived: The Babylonians, Egyptians, Indians and the Chinese knew several triples, and at least the Babylonians must have had a recipe for constructing arbitrarily many such triples almost 4000 years ago. About two millennia later, Diophantus taught how to solve “diophantine” equations that were a lot more complicated than \( x^2 + y^2 = z^2 \) in his *Arithmetica*.

The diophantine tradition was kept alive in Islamic mathematics and was rediscovered in the West at around the time when Bombelli and Vieta developed their algebra. A highly influential edition of the *Arithmetica* was published by Claude Gaspare Bachet de Méziriac in 1621. In his comments, Bachet asked which primes can be represented as sums of two squares and guessed that this is always possible if \( p \) has the form \( 4n + 1 \). Fermat developed the technique of infinite descent for his proof that sums of two coprime squares are never divisible by primes of the form \( 4n - 1 \), and later was able to prove the full conjecture. Fermat also looked at more general forms \( x^2 - Ay^2 \) for small values of \( A \), and most of his conjectures were later proved by Euler and Lagrange. Euler, in particular, distilled the quadratic reciprocity law from his investigations without being able to prove it. Observe that if \( p \) is a prime number coprime to \( 2A \) represented by the form \( x^2 - Ay^2 \), then \( A \) is a square modulo \( p \).

**Theorem 2.1** (Euler’s Version of the Quadratic Reciprocity Law). If \( p \) and \( q \) are prime numbers with \( p \equiv q \mod 4A \), then \( (\frac{A}{p}) = (\frac{A}{q}) \).

Let us give a few examples of how special cases of quadratic reciprocity were used by Fermat, Euler and Lagrange to prove results about quadratic forms.

The simplest case concerns sums of two squares. The starting point is the observation that \(-1\) is a square modulo \( p \) for primes \( p \equiv 1 \mod 4 \). Thus \( x^2 + 1 = mp \) for some integer \( m \),
and this means that there is a *multiple* of $p$ that can be represented as a sum of two squares. Fermat’s descent shows that if $m > 1$, then there is an integer $m' < m$ for which $m'$ is a sum of two squares, and this implies the Two-Squares Theorem. The descent argument is based on the observation that if $p = a^2 + b^2$, then $2p = (a + b)^2 + (a - b)^2$, and that, conversely, if $2p = c^2 + d^2$, then $c$ and $d$ are odd and we have $p = (\frac{c + d}{2})^2 + (\frac{c - d}{2})^2$. Similar results are valid for primes $q > 2$ as well.

Next consider the problem of primes represented by the form $x^2 - 2y^2$. Assume that $p \equiv \pm 1 \mod 8$; this is equivalent to $(\frac{2}{p}) = 1$, so $x^2 \equiv 2 \mod p$ has a solution. But then $x^2 - 2 = mp$ for some integer $m$, hence $mp$ is represented by the form $x^2 - 2y^2$. Now a descent argument (if $m > 1$, then there is some $m_1 < m$ with $m_1p = x_1^2 - 2y_1^2$) is used to prove that $p$ is represented by $x^2 - 2y^2$.

But, as already Fermat observed, there is trouble ahead for $A = -5$. The primes $p$ with $(\frac{-5}{p})$ are, by Euler’s (conjectured) reciprocity law, those with $p \equiv 1, 3, 7, 9 \mod 20$. Since $(\frac{-5}{p}) = (\frac{1}{p})(\frac{5}{p})$, this follows from the first supplementary law $(\frac{1}{p}) = (-1)^{\frac{p-1}{2}}$ known to Fermat and Euler, and from the special case $(\frac{5}{p}) = (\frac{p}{5})$ of the quadratic reciprocity law, which Lagrange was able to prove using an ingenious trick (Gauss presented Lagrange’s proof in his Disquisitiones [9]).

As above it follows that $x^2 + 5 = mp$ for some integer $m$, but this time the descent argument does not work and only shows that either $p$ or $2p$ is represented by $x^2 + 5y^2$. If $2p = x^2 + 5y^2$, then $x$ and $y$ must be odd, and we can write $y = v$ and $x = 2u + v$; this implies

$$2p = x^2 + 5y^2 = (2u + v)^2 + 5v^2 = 4u^2 + 4uv + 6v^2,$$

i.e.,

$$p = 2u^2 + 2uv + 3v^2.$$ 

Thus the primes $p$ with $(\frac{-5}{p}) = 1$ are represented either by $Q_0(x, y) = x^2 + 5y^2$ or by $Q_1(x, y) = 2x^2 + 2xy + 3y^2$.

**Descent for** $\Delta = -20$. Let $p \equiv 1, 3, 7, 9 \mod 20$ be a prime number. We claim that $p$ is represented by $(1, 0, 5)$ or by $(2, 2, 3)$, and we will prove this by induction. Assume therefore that the claim is true for all primes less than $p$. By the quadratic reciprocity law, $-5$ is a quadratic residue modulo $p$, hence there is an integer $x$ with $x^2 \equiv -5 \mod p$. Clearly we can choose $x$ in such a way that $|x| < \frac{p}{2}$, and this implies that $x^2 + 5 < p^2$, hence $x^2 + 5 = m_1p$ for some $m_1 < p$. If $m_1 = 1$, then $p = x^2 + 5 \cdot 1^2$, and $p$ is represented by $(1, 0, 5)$. If $m_1 > 1$, then there is a prime number $q | m_1$, and $x^2 + 5 = m_1p$ implies that $x^2 \equiv -5 \mod q$. By induction assumption, $q$ is represented by $(1, 0, 5)$ or by $(2, 2, 3)$.

In the first case

In the second case
The reduction process is essentially a repeated performance of the simple transformations

\[(x, y) \mapsto \begin{cases} x' = Cx + By, & y' = Ax + By \end{cases}\]

which are induced by the substitutions \(x \to x - y\) for the first and \(x \to y, y \to x\) for the second transformation (observe that the second transformation has determinant \(-1\)).

The basic idea behind reduction is implicit in Brouncker’s solution of the Pell equation: for finding a nontrivial solution of \(x^2 - Ny^2 = 1\), Brouncker transformed the form \((1, 0, -N)\) into a series of equivalent forms with the intent of making the coefficients of a hypothetical integral solution smaller. After finitely many steps he arrived at an equivalent form \((1, B, C)\) with the trivial solution \(x = 1, y = 0\), which gave him a nontrivial (!) integral solution of the original equation by working backwards.

**From Descent to Reduction**

Consider the linear diophantine equation \(ax + by = 1\), where \(a\) and \(b\) are coprime integers.

Among the many methods for solving this equation we choose one which does not seem to be well known (there are algorithms that perform better, but we are interested in the idea behind it), but whose essential idea goes back to Bachet. The idea is to use clever substitutions that simplify the given equation until the solution becomes trivial. Consider the example of the equation \(11x + 27y = 1\); dividing through by 11 we find that \(x + \frac{27}{11}y \approx 0\), and this suggests that \(z = x + 2y\) is small compared with \(x\) and \(y\). Thus we replace \(x\) by \(x = z - 2y\) and find, by repeating this procedure,

\[
\begin{align*}
11x + 27y &= 1 & x &= z - 2y \\
11z + 5y &= 1 & y &= u - 2z \\
z + 5u &= 1 & 
\end{align*}
\]
The substitutions on the right are chosen in such a way that the coefficients of the unknowns on the left become as small as possible. In general, if the equation in question is $ax + by = 1$ and if $a < b$, then write $b = aq + r$ with $0 \leq r < a$ and substitute $x = z - qy$; this substitution transforms the equation into $1 = az + (b - aq)y = az + by$. This new equation has positive integral coefficients for which $r < a$, so after finitely many steps we end up with an equation where one of the coefficients is 0 (or 1). In the example above, the last equation has solution $z = 1, u = 0$, and now we can work backwards and find $y = u - 2z = -2$ and $x = z - 2y = 5$. Thus $5 \cdot 11 - 2 \cdot 27 = 1$.

**Brouncker's solution of the Pell equation.** Wie Brouncker wollen wir die Gleichung $13a^2 + 1 = y^2$ betrachten. Sind $a$ und $y$ groß, folgt $y \approx a\sqrt{13}$, und wegen $3 < \sqrt{13} < 4$ ist dann $3a < y < 4a$. Wenn wir also $y = 4a - b$ setzen, so folgt

$$13a^2 + 1 = (4a - b)^2 = 16a^2 - 8ab + b^2$$

und somit

$$8ab - b^2 = 3a^2 - 1.$$  

Damit haben wir die Ausgangsgleichung $y^2 - 13a^2 = 1$ in die Gleichung $3a^2 - 8ab + b^2 = 1$ verwandelt. Die Koeffizienten sind kleiner geworden, und die triviale Lösung $b = 1, a = 0$ liefert die triviale Lösung der Ausgangsgleichung.

Division durch $b^2$ liefert $\frac{8a}{b} - 1 = 3\left(\frac{a}{b}\right)^2 - \frac{1}{b^2} \approx 3\left(\frac{a}{b}\right)^2$, also $2b < a < 3b$, und die Substitution $a = 2b + c$ ergibt

$$8(2b + c)b - b^2 = 3(2b + c)^2 - 1,$$

also

$$3b^2 + 1 = 4bc + 3c^2.$$

Eine Wiederholung dieser Rechnungen führt nun auf folgendes Schema:

<table>
<thead>
<tr>
<th>Gleichung</th>
<th>Substitution</th>
</tr>
</thead>
<tbody>
<tr>
<td>$13a^2 + 1 = y^2$</td>
<td>$y = 4a - b$</td>
</tr>
<tr>
<td>$8ab - b^2 = 3a^2 - 1$</td>
<td>$a = 2b + c$</td>
</tr>
<tr>
<td>$3b^2 + 1 = 4bc + 3c^2$</td>
<td>$b = 2c - d$</td>
</tr>
<tr>
<td>$c^2 + 1 = 8cd - 3d^2$</td>
<td>$c = 8d - e$</td>
</tr>
<tr>
<td>$3d^2 + 1 = 8de - c^2$</td>
<td>$d = 2e + f$</td>
</tr>
<tr>
<td>$4ef + 3f^2 = 3e^2 - 1$</td>
<td>$e = 2f - g$</td>
</tr>
</tbody>
</table>

Damit erhält Brouncker $f^2 - 8fg + 3g^2 = 1$ (Brouncker setzt in seiner Lösung sofort $g = 0$, benutzt also die Substitution $e = 2f$). Diese Gleichung hat die Lösung $f = 1$, und Einsetzen liefert nun nacheinander

$$e = 2, \quad c = 38, \quad b = 71, \quad a = 180, \quad y = 649$$

und damit die Lösung

$$13 \cdot 180^2 + 1 = 649^2.$$  

Brounckers Substitutionen haben die Ausgangsform $(1, 0, -13)$ nacheinander in $(1, -8, 3), (3, 4, -3), (-1, 8, -3), (-3, 8, -1), (3, -4, -3)$ und $(1, -8, 3)$ transformiert. Solche Zyklen werden später der Gaußschen Reduktionstheorie indefiniter quadratischer Formen zugrunde liegen.
Reduction. Lagrange managed to prove the following result:

**Theorem 2.3.** There are only finitely many equivalence classes of forms \((A, B, C)\) with a given discriminant \(\Delta = B^2 - 4AC\). If \(p\) is a prime number with \((\frac{2}{p}) = +1\), then there is a form with discriminant \(\Delta\) that represents \(p\).

In the case \(\Delta = -20\) there are only two reduced forms, namely \((1, 0, 5)\) and \((2, 2, 3)\). Each prime \(p\) with \((-5/p) = 1\) is represented by one of these forms, and since all odd integers represented by \((1, 0, 5)\) are \(\equiv 1 \mod 4\), it follows that \((1, 0, 5)\) represents primes \(p\) satisfying \((\frac{-1}{p}) = (\frac{5}{p}) = 1\), whereas \((2, 2, 3)\) represents the primes with \((\frac{-1}{p}) = (\frac{5}{p}) = -1\).

**Composition.** From

\[ 2(2x^2 + 2xy + 3y^2) = 4x^2 + 4xy + 6y^2 = (2x + y)^2 + 5y^2 \]

we see that if \(p \equiv 3, 7 \mod 20\) is represented by \(Q_1\), then \(2p\) is represented by \(Q_0\). If \(p\) and \(q\) are such primes, then \(2p = a^2 + 5b^2\) and \(2q = c^2 + 5d^2\), hence

\[ 4pq = (a^2 + 5b^2)(c^2 + 5d^2) = (ac - 5bd)^2 + 5(ad + bc)^2, \]

and since it is easy to see that \(ac - 5bd\) and \(ad + bc\) must be even, we conclude that \(pq\) is represented by \(Q_0\). A closer look at this situation reveals that our calculations provide us with a beautiful product formula:

\[
(2a^2 + 2ab + 3b^2)(2c^2 + 2cd + 3d^2) = \frac{1}{4}[(2a + b)^2 + 5b^2][(2c + d)^2 + 5d^2] \\
= \frac{1}{4}[(2a + b)(2c + d) - 5bd]^2 + 5[(2a + b)d + (2c + d)b]^2 \\
= (2ac - 2bd + ad + bc)^2 + 5(ad + bc + bd)^2.
\]

Similar calculations yield the set of identities

\[
Q_0(a, b)Q_0(c, d) = Q_0(ac - 5bd, ad + bc) \\
Q_0(a, b)Q_1(c, d) = Q_1(ac - 3bd, ad + 2bc + bd) \\
Q_1(a, b)Q_1(c, d) = Q_0(2ac - 2bd + ad + bc, ad + bc + bd)
\]

These identities suggest that we may compose the forms with discriminant \(\Delta = -20\), namely the principal form \(Q_0(x, y) = x^2 + 5y^2\) and the form \(Q_1 = 2x^2 + 2xy + 3y^2\), in such a way that we obtain a group law on these forms whose group table is the following:

\[
\begin{array}{c|cc}
* & Q_0 & Q_1 \\
\hline
Q_0 & Q_0 & Q_1 \\
Q_1 & Q_1 & Q_0 \\
\end{array}
\]

Observe, however, that there are at least two ways of composing \(Q_0\) with itself:

\[
(a^2 + 5b^2)(c^2 + 5d^2) = (ac - 5bd)^2 + 5(ad + bc)^2 = (ac + 5bd)^2 + 5(ad - bc)^2.
\]

Both choices lead to the composition \(Q_0 \ast Q_0 \sim Q_0\); alas, things are not as simple as these calculations suggest: As Legendre discovered, such ambiguities do lead to essentially different compositions for larger discriminants. Consider e.g. the following forms of discriminant

\[ \Delta = -20 \]
\[-4 \cdot 41: \]

\[
A = x^2 + 41y^2, \\
B = 2x^2 + 2xy + 21y^2, \\
C = 5x^2 + 6xy + 10y^2, \\
D = 3x^2 + 2xy + 14y^2, \\
E = 6x^2 + 2xy + 7y^2.
\]

Note that the form \((5, 6, 10)\) is equivalent to the reduced form \((5, 4, 9)\). Composing \(C\) with itself we find

\[C(x, y)C(z, w) = A(5zx + 3xw + 3yz + 10yw, xw - yz).\]

On the other hand, we also have

\[C(x, y)C(z, w) = C'(5xw + 5zy - 6yw, xz - 2yw)\]

for the form \(C' = (2, 6, 25)\) with discriminant \(6^2 - 8 \cdot 25 = -4 \cdot 41\). The form \(C'\) is not reduced, and the transformation \(X \mapsto X - Y\) shows that it is equivalent to

\[2(X - Y)^2 + 6(X - Y)Y + 25Y^2 = 2X^2 + 2XY + 21Y^2.\]

Thus, as Legendre observes, we have \(C * C \sim A\) as well as \(C * C \sim B\), and in fact, his composition of reduced forms gives in general two different answers.

The complete “multiplication table” for the set of reduced forms of discriminant \(-4 \cdot 41\) is given by Legendre as

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>E</td>
</tr>
<tr>
<td>B</td>
<td>B</td>
<td>A</td>
<td>C</td>
<td>E</td>
<td>D</td>
</tr>
<tr>
<td>C</td>
<td>C</td>
<td>C</td>
<td>A or B</td>
<td>D or E</td>
<td>D or E</td>
</tr>
<tr>
<td>D</td>
<td>D</td>
<td>E</td>
<td>D or E</td>
<td>A or C</td>
<td>B or C</td>
</tr>
<tr>
<td>E</td>
<td>E</td>
<td>D</td>
<td>D or E</td>
<td>B or C</td>
<td>A or C</td>
</tr>
</tbody>
</table>

This looks almost like a group table, but has two serious defects: composition is not well defined, and cancellation does not work (we have \(A * C = C\) and \(B * C = C\)).

**Open Problems.** The isolated results by Fermat, Brouncker and Euler were subsumed into a reduction theory for binary quadratic forms by Lagrange. The main problems concerning quadratic forms that were left unsolved at the end of the 18th century were the following:

- The greatest gap in Lagrange’s theory was the fact that the quadratic reciprocity law was still not proved completely, despite Legendre’s attempts in [17] and [18].
- Legendre [17] connected the number \(h\) of equivalence classes of forms with negative discriminant \(-N\) with the number of representations of \(N\) as a sum of three squares, but the corresponding formulas were far from being simple.
- The composition of forms that Legendre defined in [18] allowed him to compose two forms of the same discriminant in two different ways, and so Legendre composition does not define a group structure on the set of equivalence classes.
- Which forms represent the primes \(p\) with \((\frac{p}{\Delta}) = +1\)? The case \(\Delta = -20 = -4 \cdot 5\) above suggests that the factorization \(\Delta = \Delta_1 \cdots \Delta_r\) into prime discriminants \(\Delta_j\) and the corresponding Legendre symbols \((\Delta_j/p)\) play a central role in this problem.
All four problems were solved by Gauß in his Disquisitiones Arithmeticae [9]. At the time Gauß developed his own theory of composition, he probably had not yet seen Legendre’s book [18].

3. Gauß: Binary Quadratic Forms

When Gauß entered the University of Göttingen in 1796 in order to study mathematics, he found Legendre’s memoir [17] in the library and studied it closely. He must have found it reassuring that Legendre could not prove the existence of certain auxiliary primes that he employed in his incomplete proof of the quadratic reciprocity law, since Gauß himself had spent a year searching for a proof of a similar result. Gauß completed his proof in 1796 and now started thinking about the connections between binary quadratic forms and sums of three squares, which Legendre had exposed in his memoir. Within a few months he had found a path that would allow him to attack these conjectures, and he spent the next few years working out a theory of binary quadratic forms.

In this section we will present an outline of Gauß’s theory, except that we will consider forms \((A, B, C)\) in which \(B\) is not necessarily even, and that we will not employ Gauß’s notation \((a,b,c)\) for the form \(ax^2 + 2bxy + cy^2\) which Dedekind was still using in [7]. Another ingredient necessary for properly understanding Euler’s conjectures on cubic residues is the theory of derived forms due to Lipschitz [20], which will provide us with natural and surjective group homomorphisms from the group \(\text{Cl}(\Delta f^2)\) of equivalence classes of forms with discriminant \(\Delta f^2\) to the group \(\text{Cl}(\Delta)\).

Equivalence Classes and Reduction. Unlike Legendre, modern mathematicians are breast-fed with the concept of groups and are therefore in a much better position to see where the problems in Legendre’s composition of forms are buried. One key observation is that the form \(B\) seems to have order 2, whereas there are 5 equivalence classes. Thus if we would like to construct a group using the composition of forms, then we need an even number of classes. This may be achieved by using a finer notion of equivalence, and indeed Gauß must have realized quickly that Legendre’s conjectures on sums of three squares become a lot simpler upon slightly modifying Lagrange’s notion (1) of equivalence. Gauß called two forms *properly equivalent* if (1) holds with the stronger condition that \(ad - bc = +1\). It turns out that the forms \(C = (5, 6, 10)\) and \((5, -6, 10)\) do not belong to the same proper equivalence class, and in fact the forms in the problematic classes of \(C, D\) and \(E\) split into two equivalence classes with respect to proper equivalence, so that we have 8 equivalence classes of forms with discriminant \(-4 \cdot 41\) instead of just 5 as in Lagrange’s theory. Thus although \((A, B, C) \sim (A, -B, C) \sim (C, B, A)\) with respect to the action of \(\text{GL}_2(\mathbb{Z})\), we only have \((A, B, C) \sim (C, -B, A)\) with respect to proper equivalence.

The restriction to proper equivalence changes the theory of reduction for forms with negative discriminant only superficially; a satisfactory reduction theory for forms with positive discriminant is much more technical and was developed by Gauß. A form \((A, B, C)\) with negative discriminant is called reduced if \(|B| \leq A \leq C\), with \(B > 0\) if one of these inequalities is not strict.

**Theorem 3.1.** Each form \(Q\) with negative discriminant \(\Delta < 0\) is properly equivalent to a unique reduced form \((A, B, C)\). In addition, we have \(|A| \leq \sqrt{-\Delta}/3\).

In the case \(\Delta = -20\), we have \(|A| \leq 2\), from which it is easy to deduce that the only reduced forms are \((1, 0, 5)\) and \((2, 2, 3)\).
Composition. Despite regular claims to the contrary, the introduction of proper equivalence does not solve the problem of ambiguity in Legendre’s composition of forms. In fact, in the identities behind (2) such as (3), (4) and (5), a sign has to be chosen very carefully in order to get a unique composition up to equivalence, and for understanding this choice one has to step down into the morass of formulas that Gauss had to wade through: the proof of associativity of composition in the *Disquisitiones* involves the verification of a system of 27 equations. It goes without saying that various mathematicians tried to simplify Gauss’s theory of composition; Dirichlet and Dedekind belong to this list, as does Manjul Bhargava, who found a very compact and flexible way of writing down the necessary equations.

For each octuple \((a, b, \ldots, h)\) of integers \(a, b, \ldots, h\) Bhargava defines a cube

\[
A = \begin{pmatrix}
    a & e & f \\
    b & \cdot & \cdot \\
    g & \cdot & h \\
    c & \cdot & d
\end{pmatrix}
\]

(6)

denoted occasionally by \(A = [a, b, c, d, e, f, g, h]\). Each such cube can be sliced in three different ways, producing three pairs of \(2 \times 2\)-matrices (up-down, left-right, front-back) \(M_i\) and \(N_i\) with \(M_i = \begin{pmatrix} a & e \\ b & f \end{pmatrix}\) and \(N_i = \begin{pmatrix} c & g \\ d & h \end{pmatrix}\):

- UD: \(M_1 = U = \begin{pmatrix} a & e \\ b & f \end{pmatrix}\), \(N_1 = D = \begin{pmatrix} c & g \\ d & h \end{pmatrix}\),
- LR: \(M_2 = L = \begin{pmatrix} a & c \\ e & g \end{pmatrix}\), \(N_2 = R = \begin{pmatrix} b & d \\ f & h \end{pmatrix}\),
- FB: \(M_3 = F = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\), \(N_3 = B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}\).

To each such slicing of the cube \(A\) we can associate a binary quadratic form \(Q_i = Q_i^A\) by putting

\[
Q_i(x, y) = -\det(M_i x + N_i y).
\]

In this way we find

\[
Q_1(x, y) = (be - af)x^2 + (bg + de - ah - cf)xy + (dg - ch)y^2,
\]

(7)

\[
Q_2(x, y) = (ce - ag)x^2 + (cf + de - ah - bg)xy + (df - bh)y^2,
\]

(8)

\[
Q_3(x, y) = (bc - ad)x^2 + (bg + cf - ah - de)xy + (fg - eh)y^2.
\]

(9)

It is easily checked that all three forms have the same discriminant \(\Delta\); it requires more effort to deduce that there exists an identity

\[
Q_1(x_1, y_1)Q_2(x_2, y_2)Q_3(x_3, y_3) = Q_0(x_0, y_0),
\]

where \(Q_0\) is the principal form with discriminant \(\Delta\), and where \(x_0\) and \(y_0\) are trilinear expressions in the \(x_i\) and \(y_i\); in reminiscence of the geometric definition of the group law on elliptic curves the three forms attached to a cube are called collinear.

**Theorem 3.2.** Let \(A = [a, b, c, d, e, f, g, h]\) be a cube to which three primitive forms \(Q_i = Q_i^A\) are attached. Then

\[
Q_1(x_1, y_1)Q_2(x_2, y_2) = Q_3(x_3, -y_3),
\]

(10)
where $x_3$ and $y_3$ are linear forms in $x_1, y_1$ and $x_2, y_2$, and are given by

\[
\begin{aligned}
x_3 &= cx_1x_2 + fx_1y_2 + gx_2y_1 + hy_1y_2, \\
y_3 &= ax_1x_2 + bx_1y_2 + cx_2y_1 + dy_1y_2.
\end{aligned}
\]

As with elliptic curves, giving a direct proof of associativity remains a painful exercise despite Bhargava’s cubes. For composing forms $Q_1$ and $Q_2$ using Bhargava’s cubes one needs, of course, algorithms for computing the cube giving rise to $Q_1$ and $Q_2$, but every classical method of composition (including Gauß’s own) can be adapted to Bhargava’s cubes.

The elegant definition of composition using Bhargava’s cubes makes it difficult to see the rather mysterious choice of signs that is necessary for picking the right composition of forms from the two possibilities (4) and (5). If we compare these equations with those provided by the theorem above we find that these forms correspond to two different cubes, and that one gives rise to a different triples of forms than the other: The first composition corresponds to

\[
\begin{bmatrix}
1 & 0 & 0 \\
1 & 1 & -1 \\
3 & -10 & 5 \\
0 & 3 & 3
\end{bmatrix}
\]

with the forms $Q_1 = (-5, -6, -10)$, $Q_2 = (5, 6, 10)$, $Q_3 = (-1, 0, -41)$,

and the second to

\[
\begin{bmatrix}
1 & 0 & 0 \\
0 & 2 & -1 \\
5 & -6 & 0 \\
0 & 5 & 3
\end{bmatrix}
\]

with the forms $Q'_1 = (5, 6, 10)$, $Q'_2 = (5, 6, 10)$, $Q'_3 = (2, 6, 25)$.

Thus only the second choice leads to the right forms: there are different ways of composing forms, but only one of them is compatible with Bhargava’s cubes!

**Genus Classes.** Gauss developed his theory of binary quadratic forms in maximal generality; in fact, he even allowed the discriminant of $\Delta$ to be a square. In the following, we will sketch the main results concerning the genus theory of forms only in the special case where the discriminant $\Delta$ is fundamental, i.e., cannot be written in the form $\Delta = \Delta_1 \cdot f^2$ for a discriminant $\Delta_1$ and some integer $f$.

Each fundamental discriminant $\Delta$ can be written uniquely as a product of prime discriminants $\Delta_j$. These prime discriminants are

- $\Delta = -4$ and $\Delta = \pm 8$;
- $\Delta = p$, where $p \equiv 1 \pmod{4}$ is prime;
- $\Delta = -q$, where $q \equiv 3 \pmod{4}$ is prime.

To each form $Q$ with discriminant $\Delta = \Delta_1 \cdots \Delta_t$, pick a prime $p \nmid \Delta$ represented by $Q$, and attach to $Q$ a sign vector

\[
\chi(Q) = (\chi_1(p), \ldots, \chi_t(p)), \quad \text{where} \quad \chi_j(p) = \left( \frac{\Delta_j}{p} \right).
\]

Gauß proved that this does not depend on the choice of $p$ or on the equivalence class of $Q$. Forms $Q$ with the same vector $\chi(Q)$ are collected into a *genus* of forms. Since each genus has the same number of forms, the class number $h$ is always divisible by the number of genera.
Theorem 3.3 (Main Theorem of Genus Theory). Let \( \Delta = \Delta_1 \cdots \Delta_t \) be the factorization of a fundamental discriminant into prime discriminants. There exists a form with a given sign vector \((e_1, \ldots, e_t)\) if and only if \(e_1 \cdots e_t = +1\). In particular, exactly half of the possible genera exist, and the number of genera is \(2^{t-1}\). Finally, a form \(Q\) is contained in the principal genus with sign vector \(\chi(q) = (1, \ldots, 1)\) if and only if \(Q\) is equivalent to the square of another form.

Gauß used this result to give another proof of the quadratic reciprocity law.

Let us give a few instructive examples of what genus theory can achieve. Our first examples is \(\Delta = -84\); here \(\Delta = -4 \cdot (-3) \cdot (-7)\), hence there are 4 genera of forms. If we set \(\chi(Q) = ((\frac{-3}{p}), (\frac{-4}{p}), (\frac{-7}{p}))\), where \(p \nmid \Delta\) is a prime represented by \(q\), then we find

<table>
<thead>
<tr>
<th>condition</th>
<th>forms</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\chi(Q) = (+1,+1,+1))</td>
<td>((1,0,21))</td>
</tr>
<tr>
<td>(\chi(Q) = (+1,-1,-1))</td>
<td>((3,0,7))</td>
</tr>
<tr>
<td>(\chi(Q) = (-1,+1,-1))</td>
<td>((5,4,5))</td>
</tr>
<tr>
<td>(\chi(Q) = (-1,-1,+1))</td>
<td>((11,-2,2))</td>
</tr>
</tbody>
</table>

In our second example \(\Delta = -39\), genus theory does not suffice for separating the form classes completely. Here the class group is cyclic of order 4, and it is generated by \((2,1,5)\). With \(\chi(Q) = ((\frac{-3}{p}), (\frac{13}{p}))\) we get

<table>
<thead>
<tr>
<th>condition</th>
<th>forms</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\chi(Q) = (+1,+1))</td>
<td>((1,1,10)), ((3,3,4))</td>
</tr>
<tr>
<td>(\chi(Q) = (-1,-1))</td>
<td>((2,1,5), (2,-1,5))</td>
</tr>
</tbody>
</table>

Here the forms \((1,1,10)\) and \((3,3,4)\) cannot be separated by simple congruence conditions. We will return to this example later when we discuss what class field theory has to do with this question.

4. Derived Forms

The composition of (equivalence classes of) forms using Bhargava’s cubes works for general discriminants. Already Gauß observed (in the case of forms with negative discriminant) that the class number \(h(\Delta)\) always divides \(h(\Delta \cdot f^2)\). The actual reasons for this observation were worked out by Lipschitz [20].

It is easy to prove that each form with discriminant \(-\Delta f^2\) is equivalent to a form \((A,Bf,Cf^2)\). Mapping this form to \((A,B,C)\) with discriminant \(\Delta\) gives us a well defined surjective group homomorphism \(\text{Cl}(\Delta \cdot f^2) \rightarrow \text{Cl}(\Delta)\); of course we need to check various facts.

Since we can go from forms with discriminant \(\Delta \cdot f^2\) down to forms with discriminant \(\Delta\) in “prime steps” it is sufficient to look at the relation between \(\text{Cl}(\Delta)\) and \(\text{Cl}(\Delta \cdot p^2)\). The group structure of the kernel \(\ker \pi_2 : \text{Cl}(\Delta \cdot p^2) \rightarrow \text{Cl}(\Delta)\) can be determined explicitly, and the order of this kernel may be shown to be

\[
\frac{h(\Delta p^2)}{h(\Delta)} = \frac{p - \chi(p)}{e},
\]
where \( \chi(p) = \left( \frac{\Delta}{p} \right) \), and where \( e \) is defined, for forms with negative discriminants, by

\[
e = \frac{\text{number of solutions of } Q_\infty(T, U) = 1}{\text{number of solutions of } Q_f(T, U) = 1},
\]

where \( Q_\infty \) is the form derived from the principal form with discriminant \( \Delta \), i.e.,

\[
Q_\infty(x, y) = \begin{cases} 
  x^2 - mf^2y^2 & \text{if } \Delta = 4m, \\
  x^2 + fxy + \frac{1-m}{4}f^2y^2 & \text{if } \Delta = 4m + 1.
\end{cases}
\]

Clearly \( e = 1 \) except possibly for \( p = 2 \) or for \( \Delta = -3 \) or \( \Delta = -4 \), since the Pell equation has only the two solutions \( x = \pm 1, y = 0 \) except in the last two cases.

Thus in almost all cases (12) shows that the kernel has order \( p - \chi(p) \). This is more than superficially reminiscent of a phenomenon in the theory of elliptic curves. Given an elliptic curve \( E \) defined over the rationals we can consider its reduction \( E(\mathbb{F}_p) \) modulo a prime \( p \); this reduction may have a singular point, but the geometric group law still makes sense if we avoid the singularity. The order of the group \( E(\mathbb{F}_p) \) is \( p - 1 \), and can actually be shown to be isomorphic to the group of points on a suitably defined conic. The determination of the group structure of the kernel in the case of quadratic forms also leads to a group of points on a conic defined over the finite field \( \mathbb{F}_p \), and the close analogy may be explained by the fact that the theory of elliptic curves over a field \( K \) is nothing but a theory of binary quadratic forms over the polynomial ring \( K[T] \) since both theories can be formulated in terms of quadratic extensions of the function field \( K(T) \).

Using (12) it is now easy to compute e.g. \( h(-3f^2) \); the clas numbers for \( f \leq 25 \) are collected in Table 1.

<table>
<thead>
<tr>
<th>( f )</th>
<th>( h(-3f^2) )</th>
<th>( f )</th>
<th>( h(-3f^2) )</th>
<th>( f )</th>
<th>( h(-3f^2) )</th>
<th>( f )</th>
<th>( h(-3f^2) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>6</td>
<td>3</td>
<td>11</td>
<td>4</td>
<td>16</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>7</td>
<td>2</td>
<td>12</td>
<td>6</td>
<td>17</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>8</td>
<td>4</td>
<td>13</td>
<td>4</td>
<td>18</td>
<td>9</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>9</td>
<td>3</td>
<td>14</td>
<td>6</td>
<td>19</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>10</td>
<td>6</td>
<td>15</td>
<td>6</td>
<td>20</td>
<td>12</td>
</tr>
</tbody>
</table>

**Table 1. Class numbers \( h(-3f^2) \)**

**Forms with discriminant** \( \Delta = -12q^2 \). We have \( h(-3 \cdot 2^2) = 1 \), hence every prime \( p \equiv 1 \mod 3 \) is represented by the form \((1, 0, 3)\).

We construct the classes of forms with discriminant \( \Delta = -12p^2 \) for primes \( p \equiv 1 \mod 3 \) as follows. Set \( Q_\infty = (1, 0, 3p^2) \). Write \( p = a^2 + 3b^2 \); if \( p \nmid b \) then \( a \equiv \pm kb \mod p \), that is, \( a = kb + xq \). Then

\[
p = a^2 + 3b^2 = q^2x^2 + 2kqbx + (k^2 + 3)b^2.
\]

In particular, \( p \) is represented by the form \( Q_k = (q^2, 2kq, k^2 + 3) \). We have \( Q_r \sim Q_s \) if and only if \( r \equiv s \mod p \), hence the forms \( Q_k \) for \( k = 0, 1, \ldots, p-1 \) are not equivalent and represent the nonprincipal classes. The group law is given by \( Q_r + Q_s = Q_t \) for \( t \equiv \frac{r-s}{r+s} \mod p \).
The quartic case. For a better understanding of the situation for cubic residuacity we will also take a quick look at the corresponding problem for quartic residuacity. In this case we can prepare a table of class numbers with discriminant $\Delta = -4$.

For $q = 5$, there are the following forms.

<table>
<thead>
<tr>
<th>$k$</th>
<th>$Q_k$</th>
<th>reduced</th>
<th>$\pi_2(Q)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\infty$</td>
<td>(1, 0, 75)</td>
<td>(1, 0, 75)</td>
<td>(1, 1, 19)</td>
</tr>
<tr>
<td>0</td>
<td>(25, 0, 3)</td>
<td>(3, 0, 25)</td>
<td>(3, 3, 7)</td>
</tr>
<tr>
<td>1</td>
<td>(25, 10, 4)</td>
<td>(4, -2, 19)</td>
<td>(1, 1, 19)</td>
</tr>
<tr>
<td>2</td>
<td>(25, 20, 7)</td>
<td>(7, -6, 12)</td>
<td>(3, 3, 7)</td>
</tr>
<tr>
<td>3</td>
<td>(25, 30, 12)</td>
<td>(7, 6, 12)</td>
<td>(3, 3, 7)</td>
</tr>
<tr>
<td>4</td>
<td>(25, 40, 19)</td>
<td>(4, 2, 19)</td>
<td>(1, 1, 19)</td>
</tr>
</tbody>
</table>

$q = 11$:

<table>
<thead>
<tr>
<th>$k$</th>
<th>$Q_k$</th>
<th>reduced</th>
<th>$\pi_2(Q)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\infty$</td>
<td>(1, 0, 363)</td>
<td>(1, 0, 75)</td>
<td>(1, 1, 91)</td>
</tr>
<tr>
<td>0</td>
<td>(121, 0, 3)</td>
<td>(3, 0, 121)</td>
<td>(3, 3, 31)</td>
</tr>
<tr>
<td>1</td>
<td>(121, 22, 4)</td>
<td>(4, 2, 91)</td>
<td>(1, 1, 91)</td>
</tr>
<tr>
<td>2</td>
<td>(121, 44, 7)</td>
<td>(7, -2, 52)</td>
<td>(7, -1, 13)</td>
</tr>
<tr>
<td>3</td>
<td>(121, 66, 12)</td>
<td>(12, 6, 31)</td>
<td>(3, 3, 31)</td>
</tr>
<tr>
<td>4</td>
<td>(121, 88, 19)</td>
<td>(19, -12, 21)</td>
<td>(7, 1, 13)</td>
</tr>
<tr>
<td>5</td>
<td>(121, 110, 28)</td>
<td>(13, -2, 28)</td>
<td>(7, 1, 13)</td>
</tr>
<tr>
<td>6</td>
<td>(121, 132, 39)</td>
<td>(13, 2, 28)</td>
<td>(7, -1, 13)</td>
</tr>
<tr>
<td>7</td>
<td>(121, 154, 52)</td>
<td>(19, 12, 21)</td>
<td>(7, -1, 13)</td>
</tr>
<tr>
<td>8</td>
<td>(121, 176, 67)</td>
<td>(12, -6, 31)</td>
<td>(3, 3, 31)</td>
</tr>
<tr>
<td>9</td>
<td>(121, 198, 84)</td>
<td>(7, 2, 52)</td>
<td>(7, 1, 13)</td>
</tr>
<tr>
<td>10</td>
<td>(121, 220, 103)</td>
<td>(4, -2, 91)</td>
<td>(1, 1, 91)</td>
</tr>
</tbody>
</table>

For $q = 7$, we find that $Q_2$ and $Q_5$ are not primitive.

<table>
<thead>
<tr>
<th>$k$</th>
<th>$Q_k$</th>
<th>reduced</th>
<th>$\pi_2(Q)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\infty$</td>
<td>(1, 0, 147)</td>
<td>(1, 0, 147)</td>
<td>(1, 1, 37)</td>
</tr>
<tr>
<td>0</td>
<td>(49, 0, 3)</td>
<td>(3, 0, 49)</td>
<td>(3, 3, 13)</td>
</tr>
<tr>
<td>1</td>
<td>(49, 14, 4)</td>
<td>(4, 2, 37)</td>
<td>(1, 1, 37)</td>
</tr>
<tr>
<td>3</td>
<td>(49, 42, 12)</td>
<td>(12, 6, 13)</td>
<td>(3, 3, 13)</td>
</tr>
<tr>
<td>4</td>
<td>(49, 56, 19)</td>
<td>(12, -6, 13)</td>
<td>(3, 3, 13)</td>
</tr>
<tr>
<td>6</td>
<td>(49, 84, 39)</td>
<td>(4, -2, 37)</td>
<td>(1, 1, 37)</td>
</tr>
</tbody>
</table>

The quartic case. For a better understanding of the situation for cubic residuacity we will also take a quick look at the corresponding problem for quartic residuacity. In this case we are dealing with prime numbers $p \equiv 1 \mod 4$, which are represented by the form $x^2 + y^2$ with discriminant $-4$, and more exactly by the form $x^2 + 4y^2$ with discriminant $-4 \cdot 2^2$. As in the cubic case we can prepare a table of class numbers with discriminant $\Delta = -4f^2$.

Let us look at a few characteristic examples in detail.

- $\Delta = -4 \cdot 3^2$: the two equivalence classes are represented by the forms $(1, 0, 9)$ and $(2, 2, 5)$. The first form represents prime numbers $p \equiv 1 \mod 3$, the second form primes $p \equiv 2 \mod 3$.
- $\Delta = -4 \cdot 4^2$: the two equivalence classes are represented by the forms $(1, 0, 16)$ and $(4, 4, 5)$. The first form represents primes $p \equiv 1 \mod 8$, the second form primes $p \equiv 5 \mod 8$.

Although it is not easy to spot a pattern here, there is a simple construction of the forms representing the classes with discriminant $\Delta = -4f^2$. In the case $f = 3$, we start with the observation that primes $p \equiv 1 \mod 4$ are represented by the form $(1, 0, 1)$. Write $p = a^2 + b^2$;
For prime numbers

Proposition 4.2. sent the same primes.

The composition law is given by

\[ \text{Cl}(ab) = \text{Cl}(a) \cdot \text{Cl}(b) \]

Thus we have found two classes of forms: \( Q_\infty = (1, 0, q) \) represents primes \( p \equiv 1 \mod 12 \), \( Q_1 = (2, 2, 5) \) represents primes \( p \equiv 5 \mod 12 \).

**Discriminants** \( \Delta = -4p^2 \). Assume first that \( q \equiv 3 \mod 4 \); then \( h(-4q^2) = \frac{2q+1}{2} \). As above, write \( p = a^2 + b^2 \) and consider the cases \( q \mid ab \) and \( q \nmid ab \). The first case leads to the principal form \( Q_\infty = (1, 0, q) \) with discriminant \( \Delta = -4q^2 \). In the second case, we can write \( a = xq \pm kb \) and find

\[ p = a^2 + b^2 = (xq \pm kb)^2 + b^2 = x^2q^2 \pm 2kqxb + (k^2 + 1)b^2, \]

hence \( p \) is represented by the forms \( Q_{\pm k} = (q^2, \pm 2kq, k^2 + 1) \) with discriminant \( -4q^2 \), and conversely it is easy to see that if \( p = a^2 + b^2 \) is a form represented by \( Q_{\pm k} \), then \( a \equiv \pm k \mod b \).

It remains to determine which of the forms \( Q_{\pm k} \) are equivalent, and which form \( Q_t \) is the composition of the forms \( Q_r \) and \( Q_s \).

**Quadratic forms.** Let \( p = a^2 + 4b^2 \equiv 1 \mod 4 \) be a prime number, and fix another prime number \( q \). If \( \frac{a}{2b} \equiv k \mod q \), then \( a \equiv 2kb \mod q \) and thus \( a = qx + 2kb \) for some integer \( x \). But then

\[ p = a^2 + 4b^2 = (qx + 2kb)^2 + 4b^2 = q^2x^2 + 4bkqx + 4(k^2 + 1)b^2, \]

hence \( p \) is represented by the binary quadratic form \( Q_k = (q^2, 4kq, 4k^2 + 4) \) with discriminant \( \Delta = -16 \cdot q^2 \).

**Proposition 4.1.** The form \( Q_k(x, y) = (q^2, 4kq, 4k^2 + 4) \) with discriminant \( -16q^2 \) represents a prime number \( p = a^2 + 4b^2 \) if and only if \( a \equiv \pm 2kb \mod q \).

This agrees well with the fact that the forms \( Q_k(x, y) \) and \( Q_{-k}(x, y) \sim Q_k(x, -y) \) represent the same primes.

**Proposition 4.2.** For prime numbers \( q \), the classes of \( \text{Cl}(-16q^2) \) are represented by

\[ Q_{\infty}(x, y) = (1, 0, 4q^2) \quad \text{and} \quad Q_k = (q^2, 4kq, 4k^2 + 4), \quad 0 \leq k \leq q - 1, \quad q \nmid k^2 + 1. \]

The composition law is given by \( Q_r * Q_s = Q_t \), where

\[ t \equiv \frac{rs - 1}{r + s} \mod q. \]
For \( q = 3 \) we have the following forms

\[
\begin{array}{c|cc}
  k & \Delta = -16p^2 & \Delta = -4p^2 \\
  \infty & (1, 0, 36) & (1, 0, 9) \\
  0 & (9, 0, 4) \sim (4, 0, 9) & (9, 0, 1) \sim (1, 0, 9) \\
  1 & (9, 12, 8) \sim (5, -4, 8) & (9, 6, 2) \sim (2, 2, 5) \\
  2 & (9, 24, 20) \sim (5, 4, 8) & (9, 12, 5) \sim (2, 2, 5) \\
\end{array}
\]

Here are the forms for \( q = 7 \):

\[
\begin{array}{c|cc}
  k & \Delta = -16p^2 & \Delta = -4p^2 \\
  \infty & (1, 0, 596) & (1, 0, 49) \\
  0 & (49, 0, 4) \sim (4, 0, 49) & (49, 0, 1) \sim (1, 0, 49) \\
  1 & (49, 28, 8) \sim (8, 4, 25) & (49, 14, 2) \sim (2, 2, 25) \\
  2 & (49, 56, 20) \sim (13, -10, 17) & (49, 28, 5) \sim (5, 2, 10) \\
  3 & (49, 84, 40) \sim (5, 4, 40) & (49, 42, 10) \sim (5, 2, 10) \\
  4 & (49, 112, 68) \sim (5, -4, 40) & (49, 56, 17) \sim (5, -2, 10) \\
  5 & (49, 140, 104) \sim (13, 10, 17) & (49, 70, 26) \sim (5, -2, 10) \\
  6 & (49, 168, 148) \sim (8, -4, 25) & (49, 84, 37) \sim (2, 2, 25) \\
\end{array}
\]

\( Q_1 * Q_2 = Q_5 \)

**Lemma 4.3.** The forms \( Q_r \) and \( Q_s \) with discriminant \( \Delta = -16p^2 \) have equivalent images in \( \text{Cl}(-4p^2) \) if and only if \( rs \equiv -1 \mod p \).

### 5. Pell Conics

This section contributes little to the understanding of Dedekind’s article, but provides us with a nice interpretation of the group law of derived forms with discriminant \( \Delta = -4f^2 \).

**Group law on lines.** Consider the parabola \( P : y = x^2 - d \) for some integer \( d \). For a field \( k \), we call a point \( P(x, y) \) on the parabola \( k \)-rational (or simply rational if \( k \) is fixed) if \( x, y \in k \). Let \( \ell \) denote the set of rational points on the line \( y = 0 \), with all points \((x, 0)\) with \( x^2 = d \) removed (if there are any).

Now we define an addition of points on \( \ell \) as follows: given two points \( R(r, 0) \) and \( S(s, 0) \) we consider the points \( R^*(r, r^2 - d) \) and \( S^*(s, s^2 - d) \) on \( P \); the line \( R^*S^* \) intersects the \( x \)-axis in a point \( T(t, 0) \), and we set \( R \oplus S = T \). If \( R = S \), we replace the line \( R^*T^* \) by the tangent to the parabola at \( R^* \).

A simple calculation shows that the \( x \)-coordinate of \( T(t, 0) \) is given by

\[
t = \begin{cases} 
  \infty & \text{if } r + s = 0, \\
  \frac{rs + d}{r + s} & \text{if } r + s \neq 0.
\end{cases}
\]

### 6. Cubic Residuacity and Quadratic Forms

Let us now return to Euler’s Conjectures concerning the cubic character of 2 and 3. We will now be able to put them into a larger framework, and once we have talked about the basic arithmetic of pure cubic number fields we can finally present Dedekind’s generalization of Euler’s criteria (or rather those of Gauß, since Dedekind apparently was unaware of Euler’s work in this direction).
Theorem 6.1. Let \( p \equiv 1 \mod 3 \) be a prime number. Then 2 is a cubic residue or nonresidue modulo \( p \) according as \( p \) is represented by the quadratic form \( x^2 + 27y^2 \) or \( 4x^2 + 2xy + 7y^2 \).

This is equivalent to Euler’s result since \((4, 2, 7)\) is the reduction of \((1, 0, 3)\). The latter form is derived from \((1, 9, 27) \sim (1, 1, 7)\) as well as from \((4, 6, 3) \sim (1, 0, 3)\). In fact, the theory of derived forms presents us with surjective homomorphisms:

\[
\begin{array}{ccc}
\text{Cl}(-3) & \longrightarrow & \text{Cl}(-3) \\
\downarrow & & \downarrow \\
\text{Cl}(-3) & \longrightarrow & \text{Cl}(-3)
\end{array}
\]

where all the class groups are trivial except \(\text{Cl}(-3)\), which has order 3. The three classes of forms with discriminant \(\Delta = -3 \cdot 6^2\) are the principal form \((1, 0, 27)\) and the two forms \((4, \pm 2, 7)\) of order 3:

\[
\{(1, 0, 27), (4, \pm 2, 7)\} \longrightarrow \{(1, 1, 7)\}
\]

\[
\{(1, 0, 3)\} \longrightarrow \{(1, 1, 1)\}
\]

The diagram in Fig. 1 explains how to construct the class group \(\text{Cl}(-3 \cdot 6^2)\) from the trivial group \(\text{Cl}(-3)\).

\[
\begin{array}{c}
\Delta = -3 \\
\mathbb{Q}(\sqrt{-3})
\end{array}
\quad
\begin{array}{c}
(1, 1, 1) \\
p \equiv 1 \mod 3
\end{array}
\quad
\begin{array}{c}
\Delta = -3 \cdot 3^2 \\
\mathbb{Q}(\sqrt{2})
\end{array}
\quad
\begin{array}{c}
(1, 3, 9) \sim (1, 1, 7) \\
p \equiv 1 \mod 3
\end{array}
\quad
\begin{array}{c}
\Delta = -3 \cdot 6^2 \\
(2/p)_3 \neq 1
\end{array}
\quad
\begin{array}{c}
(4, 2, 7) \\
(2/p)_3 \neq 1
\end{array}
\quad
\begin{array}{c}
(1, 6, 36) \sim (1, 0, 27) \\
(2/p)_3 = 1
\end{array}
\quad
\begin{array}{c}
(4, -2, 7) \\
(2/p)_3 \neq 1
\end{array}
\]

Figure 1. Cubic Residuacity of 2
The fact that \((1, 1, 1)\) represents primes \(p \equiv 1 \mod 3\) is explained by the decomposition law in \(\mathbb{Q}(\sqrt{-3})\). The conjecture that the primes \(p\) represented by the form \((1, 0, 27)\) are those for which 2 is a cubic residue modulo \(p\) is also related to a decomposition law. The primes \(p \equiv 1 \mod 3\) with \((2/p)_3 = 1\) are exactly the primes splitting completely in the cubic number field \(\mathbb{Q}(\sqrt[3]{2})\); as we will see, the correct correspondence involves the abelian extension \(\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})/\mathbb{Q}(\sqrt{-3})\).

The connection between the representation of a prime \(p\) by a form in \(\text{Cl}(\Delta')\) and the decomposition of \(p\) in the cubic extension \(\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})/\mathbb{Q}(\sqrt{-3})\) is provided by class field theory. It is therefore not surprising that Euler was unable to “confirm this observation by a proof”. Before we discuss what Dedekind was doing let us spend some more time on Euler’s and Gauß’s remaining criteria for the cubic residuacity of 3 and 6.

**Cubic Residuacity of 3.** In [12], Gauß stated the following theorem concerning the cubic character of 3:

**Theorem 6.2.** 3 is a cubic residue modulo some prime \(p \equiv 1 \mod 3\) if \(p\) is represented by the forms \((1, 0, 243)\) or \((4, 2, 61)\), and a nonresidue if \(p\) is represented by \((7, 6, 36)\) or \((9, 6, 28)\).

Although both Euler and Gauß used forms with discriminant \(\Delta' = -3 \cdot 18^2\), forms with discriminant \(\Delta = -3 \cdot 9^2\) would have sufficed. This was not an option for Gauß, however, who insisted on forms \((A, B, C)\) with even middle coefficients.

![Figure 2. Cubic Residuacity of 3](image)

**Cubic Residuacity of 6 and 12.** Since the class group of forms with discriminant \(-3 \cdot 18^2\) “contains” (as homomorphic images) the class groups with discriminants \(-3 \cdot 9^2\) and \(-3 \cdot 6^2\), we expect that the representability of primes by forms in \(\text{Cl}(\Delta')\) is related to the cubic character of both 2 and 3. The commutative diagram provided by the theory of derived forms is
The General Result. Now we are finally in a position to explain Dedekind’s general result, which contains all the partial conjectures and results by Euler and Gauss as special cases:

**Theorem 6.3.** Let $a, b$ be natural numbers and assume that $ab > 1$ is squarefree. Set $k = ab$ or $k = 3ab$ according as $a^2 - b^2 \equiv 0 \mod 9$ or not. Then the number of quadratic forms $(A, B, C)$ with discriminant $D = B^2 - 4AC = -3k^2$ is always a multiple of $3$, and a third of the classes of forms with this discriminant forms a subgroup $G''$ of the class group which is characterized by the following property: If $p \equiv 1 \mod 3$ is a prime number not dividing $D$, then the $k''$ forms of the subgroup $G''$ represent exactly those primes $p$ of which $ab^2$ is a cubic residue, whereas the forms of the other $2k''$ classes represent exactly those primes of which $ab^2$ is a cubic nonresidue.

7. Pure Cubic Number Fields

Just as the sign vector $\chi(Q)$ of a quadratic form tells us how a prime $p$ represented by $Q$ splits in the quadratic number fields $Q(\sqrt{2})$, the primes $p$ for which $2$ or $3$ is a cubic residue are exactly those primes that split completely in the pure cubic number field $Q(\sqrt[3]{2})$ and $Q(\sqrt[3]{3})$, respectively. It is therefore natural to look at the arithmetic of pure cubic fields for further inspiration.
The classes of number fields that had been studied extensively by 1900 were mainly cyclotomic and quadratic number fields. Thus Dedekind had to develop the theory of pure cubic number fields ab ovo. Let \( K = \mathbb{Q}(\sqrt[3]{m}) \) be a pure cubic number field. We may assume that \( m > 1 \) is cubefree, which implies that \( m \) may be written uniquely in the form \( m = ab^2 \) for squarefree natural numbers \( a \) and \( b \). Since \( \mathbb{Q}(\sqrt[3]{m}) = \mathbb{Q}(\sqrt[3]{m^2}) \), the correspondence between pure cubic number fields and pairs of natural numbers \((a, b)\) is bijective if we assume that \( a > b \). Dedekind’s first goal is the determination of an integral basis and the discriminant of \( K \).

It is easy to see that the discriminant \( D = \text{disc}_K \) has the form \( D = -3k^2 \) for some integer \( k | 3ab \). The prime numbers \( p \) dividing \( ab \) ramify completely in \( \mathcal{O}_K \), whereas the prime number 3 behaves in a more complicated manner ([7, p. 156]):

**Theorem 7.1.** The decomposition of the prime number 3 in \( K = \mathbb{Q}(\sqrt[3]{m}) \), where \( m = ab^2 \) for squarefree numbers \( a \) and \( b \), is given by

\[
3\mathcal{O}_K = \begin{cases} 
   p^3 & \text{if } a^2 \equiv b^2 \mod 9, \\
   pq^2 & \text{if } a^2 \equiv b^2 \mod 9.
\end{cases}
\]

Dedekind calls \( K \) of the first and of the second kind according as \( 9 \nmid (a^2 - b^2) \) or \( 9 \mid (a^2 - b^2) \).

The decomposition of 3 into prime ideals is used for finding the integral basis ([7, p. 161–162]):

**Theorem 7.2.** Let \( m = ab^2 \) and set \( \alpha = \sqrt[3]{ab^2} \) and \( \beta = \sqrt[3]{a^2b} \). Then

\[
\mathcal{O}_K = \begin{cases} 
   \{1, \alpha, \beta\} & \text{if } K \text{ is of the first kind}, \\
   \{1, \alpha, \frac{1+a^2+b^2}{3}\} & \text{if } K \text{ is of the second kind}.
\end{cases}
\]

The discriminant is given by \( D = -3(3ab)^2 \) in the first and \( D = -3(ab)^2 \) in the second case.

Finally, Dedekind completes the statement of the decomposition law by proving the following

**Theorem 7.3.** Let \( K = \mathbb{Q}(\sqrt[3]{m}) \) be a pure cubic number fields and \( p \nmid D \) a prime number. Then

\[
p\mathcal{O}_K = \begin{cases} 
   pq & \text{if } p \equiv 2 \mod 3, \\
   p^2q & \text{if } p \equiv 1 \mod 3, (m/p)_3 = 1, \\
   p & \text{if } p \equiv 1 \mod 3, (m/p)_3 \neq 1.
\end{cases}
\]

Here \((m/p)_3 = 1 \text{ or } \neq 1\) according as \( m \) is a cubic residue modulo \( p \) or not.

8. Class Field Theory

Now that we have a general theorem linking quadratic forms with discriminant \( \Delta = -3f^2 \) to a cubic number field with discriminant \( \Delta \) it is time to ask how we can (and how Dedekind could) prove this result.

Dedekind’s approach is difficult to understand. We will therefore explain the modern point of view and then go back and have a closer look at what Dedekind did.

**Class fields.** The connection between class groups and number fields is of course provided by class field theory. The key idea of this correspondence can already be found in Hilbert’s work, who developed class field theory for quadratic extensions and formulated a program for obtaining general unramified abelian extensions that was subsequently realized by Furtwängler in a series of articles in the early 1900s.
Cyclotomic fields. The abelian extensions of the rational number field are ramified (and, by the theory of Hilbert class fields, must be, since $\mathbb{Q}$ has class number 1), but they can be described in terms of the residue class groups: the field of $m$-th roots of unity has Galois group $(\mathbb{Z}/m\mathbb{Z})^\times$, and a prime $p \nmid f$ splits completely if and only if $p$ lies in the unit residue class.

According to the Theorem of Kronecker and Weber, every abelian extension of $\mathbb{Q}$ is contained in some cyclotomic field. In particular, the quadratic number field $K$ with discriminant $\Delta$ is contained in $\mathbb{Q}(\zeta_m)$ with $m = |\Delta|$. To this subextension there corresponds a subgroup $H_{\Delta}$ of index 2 in $(\mathbb{Z}/m\mathbb{Z})^\times$, and the primes splitting in $K/\mathbb{Q}$ are exactly those whose residue classes are contained in $H$.

As an example, consider the field $\mathbb{Q}(\zeta_{15})$ of 15th roots of unity. The Galois group $G$ of $\mathbb{Q}(\zeta_{15})/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/15\mathbb{Z})^\times \simeq (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$; we have listed the subgroups of $G$ as well as their corresponding fixed fields. The residue classes $1, 4, 7, 13 \mod 15$ of the group associated to $\mathbb{Q}(\sqrt{-3})$ are exactly the residue classes modulo 15 that are represented by elements $\equiv 1 \mod 3$. The residue classes that are represented by elements $\equiv 1 \mod 5$ form the group corresponding to $\mathbb{Q}(\zeta_5)$.

The situation is reminiscent of the one for quadratic forms above: there are natural homomorphisms between these residue class groups since residue classes modulo 15 may always be projected down to residue classes modulo 3 and modulo 5:

---

**Figure 3. Cyclotomic Fields**

<table>
<thead>
<tr>
<th>$F$</th>
<th>$\mathcal{H}$</th>
<th>$\text{Gal}(F/\mathbb{Q})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Q}(\zeta_m)$</td>
<td>$1 + m\mathbb{Z}$</td>
<td>$(\mathbb{Z}/m\mathbb{Z})^\times$</td>
</tr>
<tr>
<td>$\mathbb{Q}(\sqrt{\Delta})$</td>
<td>$H_{\Delta}$</td>
<td>$\mathbb{Z}/2\mathbb{Z}$</td>
</tr>
<tr>
<td>$\mathbb{Q}$</td>
<td>$(\mathbb{Z}/m\mathbb{Z})^\times$</td>
<td>1</td>
</tr>
</tbody>
</table>

**Figure 4. Subfields of the cyclotomic field $\mathbb{Q}(\zeta_{15})$**

The situation is reminiscent of the one for quadratic forms above: there are natural homomorphisms between these residue class groups since residue classes modulo 15 may always be projected down to residue classes modulo 3 and modulo 5:
Hilbert class fields. Hilbert realized that the maximal abelian unramified extension $K^1/K$ of a number field $K$ is described by its class group $\text{Cl}(K)$; in particular $\text{Cl}(K) \cong \text{Gal}(K^1/K)$, and the subextensions $L/K$ of $K^1/K$ correspond bijectively to subgroups $H$ between $H_K$ and $I_K$. Moreover, the prime ideals that split completely in $L/K$ are exactly the prime ideals lying in $H$; in particular, a prime ideal splits in $K^1/K$ if and only if it is principal.

Gauß’s genus theory has a natural interpretation in Hilbert’s class field theory. To the factorization of the discriminant $\Delta = \Delta_1 \cdots \Delta_t$ of a quadratic number fields there corresponds the genus field $K_{\text{gen}} = \mathbb{Q}(\sqrt{\Delta_1}, \ldots, \sqrt{\Delta_t})$, the group $I_K^2$ of square ideals generates $\text{Cl}(K)^2$, and the prime ideals of $K$ that split completely in $K_{\text{gen}}/K$ are exactly the prime ideals whose classes lie in $\text{Cl}(K)^2$.

\[
\begin{array}{cccc}
F & \mathcal{H} & \mathcal{H}/H_K & \text{Gal}(F/K) \\
K^1 & \overset{\cong}{\longleftrightarrow} & H_K & 1 & \text{Cl}(K) \\
& & \downarrow & & \\
K_{\text{gen}} & \overset{\cong}{\longleftrightarrow} & I_K^2 H_K & \text{Cl}(K)^2 & \text{Cl}(K)/\text{Cl}(K)^2 \\
& & \downarrow & & \\
& & \overset{\cong}{\longleftrightarrow} & 1 & \text{Cl}(K) \\
K & & & \text{Gal}(F/K) \\
\end{array}
\]

Figure 5. Hilbert Class Fields

Thus if $K$ is a complex quadratic number field with class number $h = 2$, such as $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-13})$, then its discriminant $\Delta = \Delta_1 \Delta_2$ has two factors, the extension $\mathbb{Q}(\sqrt{\Delta_1}, \sqrt{\Delta_2}) = K(\sqrt{\Delta})$ is unramified (and abelian, of course), so in this case the genus class field $K_{\text{gen}}$ coincides with the full Hilbert class field $K^1$. Since $\Delta_1 = -4$ in the cases at hand, the primes splitting completely in $K^1/K$ are exactly those whose norms are $\equiv 1 \pmod{4}$. This in turn means that the primes $p$ with $\left(\frac{\Delta}{p}\right) = +1$ that are represented by the principal forms $(1,0,5)$ and $(1,0,13)$, respectively, are those satisfying the additional condition $p \equiv 1 \pmod{4}$.

Similarly, for fields such as $K = \mathbb{Q}(\sqrt{-41})$, where the class number 4 coincides with the number of genera, the Hilbert class field is just the genus class field $K_{\text{gen}} = \mathbb{Q}(i, \sqrt{-3}, \sqrt{-7})$ coming from the factorization $\Delta = -84 = -4 \cdot (-3) \cdot (-7)$ of the discriminant into prime discriminants. In particular, the representability of primes $p$ with $\left(\frac{-41}{p}\right)$ by quadratic forms with discriminant $\Delta = -84$ can be decided by evaluating the Legendre symbols $\left(\frac{-3}{p}\right)$ and $\left(\frac{-7}{p}\right)$.

For an example where $K^1$ is strictly bigger than the genus field consider $\mathbb{Q}(\sqrt{-17})$, whose class group is cyclic of order 4. The classes of the form class group are represented by the principal form $Q_0 = (1, 0, 17)$, the ambiguous form $Q_1 = (2, 2, 9)$, and the two forms $Q_2 = (3, 2, 6)$ and $Q_3 = (3, -2, 6)$. Clearly the forms $Q_0$ and $Q_1$ represent primes $\equiv 1 \pmod{4}$,
whereas $Q_2$ and $Q_3$ represent only primes $\equiv 3 \mod 4$. This corresponds to the fact that the
genus class field of $K$ is $K_{\text{gen}} = K(i) = \mathbb{Q}(i, \sqrt{17})$.

The question which forms are represented by $Q_0$ and which by $Q_1$ cannot be decided
using simple congruence conditions. It can be shown that the Hilbert class field is given
by $K_1 = K(i, \sqrt{1+4i})$, and so $(1, 0, 17)$ represents only the primes splitting completely in
$K_1/K$; if we write $p = a^2 + 4b^2$, then these primes can be characterized as those satisfying
$[\frac{1+4i}{a+2bi}] = +1$, where $[\cdot]$ is the quadratic residue symbol in $\mathbb{Z}[i]$. By the quadratic reciprocity
law in $\mathbb{Z}[i]$, we have $[\frac{1+4i}{a+2bi}] = [\frac{a+2bi}{1+4i}] = [\frac{2+4bi}{1+4i}] = (\frac{2}{17})[\frac{2a-b}{17}] = (\frac{2a-b}{17})^\frac{1}{2}$.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$a$</th>
<th>$b$</th>
<th>$(\frac{2a-b}{p})$</th>
<th>representation</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>3</td>
<td>1</td>
<td>-1</td>
<td>$Q_1(2, -1)$</td>
</tr>
<tr>
<td>53</td>
<td>7</td>
<td>1</td>
<td>+1</td>
<td>$Q_0(6, 1)$</td>
</tr>
<tr>
<td>89</td>
<td>5</td>
<td>4</td>
<td>-1</td>
<td>$Q_1(1, 3)$</td>
</tr>
<tr>
<td>101</td>
<td>1</td>
<td>5</td>
<td>-1</td>
<td>$Q_1(5, -3)$</td>
</tr>
<tr>
<td>137</td>
<td>11</td>
<td>2</td>
<td>-1</td>
<td>$Q_1(4, 3)$</td>
</tr>
<tr>
<td>149</td>
<td>7</td>
<td>5</td>
<td>+1</td>
<td>$Q_0(9, 2)$</td>
</tr>
<tr>
<td>157</td>
<td>11</td>
<td>3</td>
<td>+1</td>
<td>$Q_0(2, 3)$</td>
</tr>
</tbody>
</table>

Ray class groups. Takagi’s class field theory combines these two basic examples. The abelian
extensions of a number field may be described in a completely analogous way by generalized
class groups. In fact, let $m$ be an integral ideal in $K$ (if $K$ is not totally complex, one also has
to take infinite primes into account), let $D_K \{m\}$ denote the group of all ideals coprime to $m$
and $H_1 \{m\}$ its subgroup of principal ideals generated by elements of the form $\alpha \equiv 1 \mod m$.
The group $Cl_K \{m\} = D_K \{m\}/H_1 \{m\}$ is called the ray class group defined modulo $m$. The
usual ideal class group corresponds to $m = 1$.

<table>
<thead>
<tr>
<th>$F$</th>
<th>$H$</th>
<th>$\text{Gal}(F/K)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K^1 {m}$</td>
<td>$H {m}$</td>
<td>$Cl^1 {m}$</td>
</tr>
<tr>
<td>$K^1 {m}$</td>
<td>$H {m}$</td>
<td>$Cl^1 {m}$</td>
</tr>
<tr>
<td>$K^1 {m}$</td>
<td>$H {m}$</td>
<td>$Cl(K)$</td>
</tr>
<tr>
<td>$K$</td>
<td>$I_m$</td>
<td>$1$</td>
</tr>
</tbody>
</table>

Figure 6. Ray Class Fields

Class field theory predicts the existence of a class field $K^{(m)}$ of $K$ with the following
properties:

- $K^{(m)}/K$ is abelian with $\text{Gal}(K^{(m)}/K) \simeq Cl_K \{m\}$.
- The extension $K^{(m)}/K$ is unramified except possibly for prime ideals $p \mid m$.
- The prime ideals $p \mid m$ that split completely are exactly the prime ideals lying in the
  principal class $H^1_K \{m\}$. More generally, the inertia degree of $p$ in $K^{(m)}/K$ is equal
to the order of the ideal class $[p]$ generated by $p$ in $Cl_K \{m\}$. 
Ring class groups. For understanding Dedekind’s work we need a special class of generalized class groups called ring class groups. These ring class groups are defined modulo \( f \), where \( f \geq 1 \) is an integer. For a number field \( K \) with ring of integers \( O \) we define

- the order \( O_f = \{ \alpha \in O : \alpha \equiv z \mod f, \ z \in \mathbb{Z}, \ \gcd(z, f) = 1 \} \);
- the group of ideals \( H_z(f) = \{ (\alpha) : \alpha \equiv z \mod f, \ z \in \mathbb{Z}, \ \gcd(z, f) = 1 \} \);
- the group of principal ring ideals \( H_1(f) = \{ (\alpha) : \alpha \equiv 1 \mod f \} \);
- the group \( H(f) = \{ (\alpha) : (\alpha, f) = 1 \} \);
- the group \( D_f \) of all nonzero ideals coprime to \( f \);
- the unit group \( E_f = O_f^\times = O_f \cap \mathcal{O}_K \) of \( O_f \);
- the group \( E_f^1 = \{ \varepsilon \in E_f : \varepsilon \equiv 1 \mod f \} \) of 1-units.

The groups \( D_f/H_z((f)) \) are called ring class groups, and their order is given by

\[
(D_f : H_z((f))) = h_K \cdot \frac{\Phi(f)}{\phi(f)} \cdot (E : E_f),
\]

where \( \Phi(m) = \#((O/(f))^\times) \) is the number of coprime residue classes modulo \( f \) in \( O \). By class field theory, the ring class field \( K_f \) associated to \( H_f \) is a subfield of the ray class field modulo \( f \).

The order of the ring class group follows from the exact sequence (Cox [6, Ex. 7.30]):

\[
1 \rightarrow \{ \pm 1 \} \rightarrow (\mathbb{Z}/f\mathbb{Z})^\times \times O^\times \rightarrow (O/fO)^\times \rightarrow H/H_z(f) \rightarrow 1.
\]

If \( K \) is a complex quadratic number field with discriminant \( \Delta < 0 \), then the ring class group modulo \( f \), where \( f \) is an integer, is isomorphic to the class group \( Cl(\Delta f^2) \) of forms with discriminant \( \Delta f^2 \).

Galois theoretic characterizations. It is possible to characterize the genus class fields and the ring class fields of quadratic number fields in a purely Galois theoretic manner. The prototype of such results is the Theorem of Kronecker-Weber, according to which every abelian extension of \( \mathbb{Q} \) is contained in a cyclotomic field.

**Proposition 8.1.** An unramified abelian extension \( L/K \) of a quadratic number field is contained in the genus class field \( K_{gen} \) of \( K \) if and only if \( L/\mathbb{Q} \) is normal with an abelian \( 2 \)-elementary Galois group.

The next result may be found in Jensen [14] and Bruckner [3]:

**Proposition 8.2.** An abelian extension \( L/K \) of a quadratic number field is contained in the ring class field \( K_{gen} \) of \( K \) if and only if \( L/\mathbb{Q} \) is normal with Galois group \( G \), where \( G \) is a group extension

\[
1 \rightarrow A \rightarrow G \rightarrow g \rightarrow 1
\]

of an abelian group \( A \) with the group \( g = \langle \tau \rangle \) of order 2 such that \( \tau \sigma \tau^{-1} = \sigma^{-1} \) for any preimage \( \tau \in G \) of \( \tau \).

**Examples of ring class fields.** Table 1 gives the orders of ring class groups of \( \mathbb{Q}(\sqrt{-3}) \) modulo \( f \) for small values of \( f \). Before we discuss those examples that we are mainly interested in, namely the class numbers divisible by 3, let us give a few examples of ring class fields corresponding to even class numbers.

- We have \( h(-3 \cdot 4^2) = 2 \); the classes of \( Cl(-3 \cdot 4^2) \) are represented by \((1, 0, 12)\) and \((3, 0, 4)\), and it is obvious that the first form only represents primes \( p \equiv 1 \mod 4 \), the second only primes \( p \equiv 3 \mod 4 \). In fact, the associated ring class field is \( K(i) \).
• In a similar way it may be checked that \( K(\sqrt{5}) \) is the quadratic extension contained in the ring class field for \( f = 5 \) and \( f = 10 \), and that it is \( K(\sqrt{-7}) \) for \( f = 7 \). The ring class field for \( f = 8 \) is \( K(\zeta_8) = K(i, \sqrt{2}) \).

• The ring class field for \( f = 11 \) is a quartic cyclic extension of \( K \) ramified only at 11. Its quadratic subextension is \( K(\sqrt{-11}) = \mathbb{Q}(\sqrt{-3}, \sqrt{-11}) \) and it may be verified that the whole ring class field is given by \( L = K(\sqrt{11} + 2\sqrt{33}) \). Similarly, \( K(\sqrt{-13 + 2\sqrt{13}}) \) is the ring class field modulo 13 for \( \mathbb{Q}(\sqrt{-3}) \).

### 9. A QUESTION ON MERSENNE PRIMES

In this section we investigate the representation of prime numbers by quadratic forms with discriminant \(-7 \cdot 2^m\). Since \( h(-7 \cdot 2^2) = 1 \), all primes \( p \) with \( (\frac{-7}{p}) = +1 \) (these are \( p \equiv 1, 2, 4 \mod 7 \)) are represented by the form \((1, 0, 7)\).

The classes in \( \text{Cl}(-7 \cdot 4^2) \) are represented by the principal form \((1, 0, 28)\) and \((4, 0, 7)\); the principal form represents primes \(\equiv 1 \mod 4\), the second one primes \(\equiv 3 \mod 4\).

Climbing another rung on our ladder of derived forms we find that \( \text{Cl}(-7 \cdot 8^2) \) has order 4 and is isomorphic to Klein’s four-group. The forms representing the classes are \( Q_0 = (1, 0, 112), Q_1 = (7, 0, 16), Q_2 = (4, 4, 29) \) and \( Q_3 = (11, 6, 11) \). Here \( Q_0 \) and \( Q_2 \) are derived from \((1, 0, 28)\) either directly or via \((1, 2, 29) \sim (1, 0, 28)\). Here we have the following criteria for representation:

<table>
<thead>
<tr>
<th>form</th>
<th>condition ( p \equiv )</th>
<th>splits in</th>
</tr>
</thead>
<tbody>
<tr>
<td>((1, 0, 112))</td>
<td>(1 \mod 8)</td>
<td>(K(i, \sqrt{2}))</td>
</tr>
<tr>
<td>((11, 6, 11))</td>
<td>(3 \mod 8)</td>
<td>(K(\sqrt{-2}))</td>
</tr>
<tr>
<td>((4, 4, 29))</td>
<td>(5 \mod 8)</td>
<td>(K(i))</td>
</tr>
<tr>
<td>((7, 0, 16))</td>
<td>(7 \mod 8)</td>
<td>(K(\sqrt{2}))</td>
</tr>
</tbody>
</table>

This table is easily explained by the fact that the ring class field \( L \) for \( \text{Cl}(-7 \cdot 8^2) \) is obtained by adjoining an 8th root of unity: we have \( L = K(\zeta_8) \).

The ring class group \( \text{Cl}(-7 \cdot 16^2) \) has type \((2, 4)\); for finding a generator of the ring class field \( L/K \) we first determine the quadratic subextension of \( K(\zeta_8)/K \) over which \( L \) is cyclic.

The class group \( \text{Cl}(-7 \cdot 6^2) \) has two cyclic subgroups \( H_1 \) and \( H_2 \) of order 4, and another subgroup \( H_3 \) of order 4 isomorphic to Klein’s four group. We have

- \( H_1 = \langle [(1, 0, 448)], [(11, 10, 43)], [(4, 4, 113)], [(11, -10, 43)] \rangle \)
- \( H_2 = \langle [(1, 0, 448)], [(16, 8, 29)], [(4, 4, 113)], [(16, -8, 29)] \rangle \)
- \( H_3 = \langle [(1, 0, 448)], [(4, 4, 113)], [(7, 0, 64)], [(23, 18, 23)] \rangle \)

<table>
<thead>
<tr>
<th>( Q )</th>
<th>reduced</th>
<th>derived from</th>
</tr>
</thead>
<tbody>
<tr>
<td>((1, 0, 448))</td>
<td>((1, 0, 448))</td>
<td>((1, 0, 112))</td>
</tr>
<tr>
<td>((4, 4, 113))</td>
<td>((4, 4, 113))</td>
<td>((1, 0, 112))</td>
</tr>
<tr>
<td>((16, 8, 29))</td>
<td>((16, 8, 29))</td>
<td>((4, 4, 29))</td>
</tr>
<tr>
<td>((16, 24, 37))</td>
<td>((16, -8, 29))</td>
<td>((4, 4, 29))</td>
</tr>
<tr>
<td>((64, 0, 7))</td>
<td>((7, 0, 64))</td>
<td>((7, 0, 16))</td>
</tr>
<tr>
<td>((64, 32, 11))</td>
<td>((11, -10, 43))</td>
<td>((11, 6, 11))</td>
</tr>
<tr>
<td>((64, 64, 23))</td>
<td>((23, 18, 23))</td>
<td>((7, 0, 16))</td>
</tr>
<tr>
<td>((64, 96, 43))</td>
<td>((11, 10, 43))</td>
<td>((11, 6, 11))</td>
</tr>
</tbody>
</table>
The corresponding ring class field is generated by a square root of $2 + 3\sqrt{2}$ over $K(\zeta_8)$.

The two nonequivalent forms derived from $(1, 0, 112)$ are $Q_0 = (1, 0, 448)$ and $Q_4 = (4, 4, 113)$. The principal form represents primes that split completely in $L$, the other one those whose decomposition field is $K(\zeta_8)$. For getting an explicit description of the decomposition law we write $p = e^2 - 2f^2$ and assume that $e, f > 0$; since $p \equiv 1 \mod 8$ we know that $2 | f$ and $(\frac{\pi}{p}) = 1$. With $\pi = e + f\sqrt{2}$ we have $f\sqrt{2} \equiv -e \mod \pi$. Writing $f = 2^i u$ for some odd integer $u$ we then have $(\frac{\pi}{p}) = (\frac{2^i u}{p}) = (\frac{2}{p}) = +1$ since $p = e^2 - 2f^2 \equiv e^2 \mod f$ and therefore also modulo $u$. Thus

$$\frac{2 + 3\sqrt{2}}{e + f\sqrt{2}} = \left[ \frac{f}{\pi} \right] \frac{2f + 3\sqrt{2}}{e + f\sqrt{2}} = \left( \frac{f}{p} \right) \frac{2f - 3e}{\pi} = \left( \frac{2f - 3e}{p} \right)$$

$$= \left( \frac{3e - 2f}{p} \right) = \left( \frac{p}{33 - 2f} \right) = \left( \frac{e^2 - 2f^2}{3e - 2f} \right) = \left( \frac{-14}{3e - 2f} \right).$$

Here we have used the following facts:

- $2f - 3e < 0$: this follows from $4f^2 - 2e^2 = -2p < 7e^2$.
- $2(e^2 - 2f^2) \equiv 2e^2 - 4f^2 - (3e - 2f)(3e + 2f) = -7e^2 \mod (3e - 2f)$ implies that $(\frac{e^2 - 2f^2}{3e - 2f}) = (\frac{2}{3e - 2f})(\frac{-7}{3e - 2f}) = (\frac{-14}{3e - 2f})$.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$e$</th>
<th>$f$</th>
<th>$\left( \frac{-14}{3e - 2f} \right)$</th>
<th>represented by</th>
</tr>
</thead>
<tbody>
<tr>
<td>113</td>
<td>11</td>
<td>2</td>
<td>$-1$</td>
<td>$Q_4(1, -1)$</td>
</tr>
<tr>
<td>137</td>
<td>13</td>
<td>4</td>
<td>$-1$</td>
<td>$Q_4(3, -1)$</td>
</tr>
<tr>
<td>193</td>
<td>15</td>
<td>4</td>
<td>$-1$</td>
<td>$Q_4(5, -1)$</td>
</tr>
<tr>
<td>233</td>
<td>19</td>
<td>8</td>
<td>$-1$</td>
<td>$Q_4(6, -1)$</td>
</tr>
<tr>
<td>281</td>
<td>17</td>
<td>2</td>
<td>$-1$</td>
<td>$Q_4(7, -1)$</td>
</tr>
<tr>
<td>337</td>
<td>27</td>
<td>14</td>
<td>$-1$</td>
<td>$Q_4(8, -1)$</td>
</tr>
<tr>
<td>401</td>
<td>23</td>
<td>8</td>
<td>$-1$</td>
<td>$Q_4(9, -1)$</td>
</tr>
<tr>
<td>449</td>
<td>31</td>
<td>16</td>
<td>$+1$</td>
<td>$Q_6(1, 1)$</td>
</tr>
<tr>
<td>457</td>
<td>23</td>
<td>6</td>
<td>$+1$</td>
<td>$Q_6(3, 1)$</td>
</tr>
</tbody>
</table>

Thus Mersenne primes $M_p$ with $p \equiv 3 \mod 4$ must be represented either by $Q_1 \sim (16, 0, 7)$ or by $Q_3 \sim (4, 8, 11)$. Since $Q_3$ only represents primes $\equiv 7, 11 \mod 16$ we find that the $M_p$ with $p \equiv 3 \mod 4$ are represented by $Q_1$.

Consider Mersenne primes $M_p = 2^p - 1$ for primes $p \geq 3$. If $p \equiv 3 \mod 4$, then $M_p \equiv 1 \mod 7$, and if $M_p$ is prime, then it is represented by the quadratic form $x^2 + 7y^2$ with discriminant $-7 \cdot 2^2$. There are two equivalence classes of forms with discriminant $-7 \cdot 4^2$, namely $Q_0 = (1, 0, 28)$ and $Q_1 = (4, 0, 7)$. The form $Q_0$ only represents primes $\equiv 1 \mod 4$, so the Mersenne primes must be represented by $Q_1$.

The following table presents the first few values of $x$ and $y$ with $M_p = 16x^2 + 7y^2$:

<table>
<thead>
<tr>
<th>$p$</th>
<th>$x$</th>
<th>$y$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>19</td>
<td>180</td>
<td>29</td>
</tr>
<tr>
<td>31</td>
<td>10992</td>
<td>5533</td>
</tr>
</tbody>
</table>

This table suggests that the values of $x$ are all even, i.e., that $M_p$ is represented by the form $(64, 0, 7)$ with discriminant $-7 \cdot 16^2$; the other form in $\text{Cl}(-7 \cdot 16^2)$ derived from $Q_1$ is $(64, 64, 23) \sim (23, 18, 23)$. 
10. Pure cubic fields as class fields

The situation in the cubic case is more complex because in this case, the class field is not abelian over the rationals. In fact, cyclic cubic extensions \( L/K \) of \( K = \mathbb{Q}(\sqrt[3]{-3}) \) correspond to generalized ideal class groups of order 3. By Kummer theory we know that cyclic cubic extensions \( L/K \) are Kummer extensions, that is, they have the form \( L = K(\sqrt[3]{\mu}) \) for some \( \mu \in K^\times \). If the defining modulus \( m \) is invariant under the action of the Galois group of \( \text{Gal}(K/\mathbb{Q}) \), then \( L/\mathbb{Q} \) is normal, and the Galois group is the dihedral group of order 6, usually denoted by \( S_3 \). This implies that the generator \( \mu \) may be chosen rational, that is, we have \( L = K(\sqrt[3]{m}) \) for an integer \( m \). In particular this happens if the defining modulus \( m = (f) \) is an integer. In this case we have already observed that the ray class group modulo \( f \) is isomorphic to the class group of forms with discriminant \( \Delta = -3f^2 \).

Assume that this class group \( \text{Cl}(-3f^2) \) has order divisible by 3, let \( H \) be a subgroup of index 3, let \( \mathcal{H} \) denote the corresponding ideal group in \( k \) defined modulo \( f \), and let \( F = \mathbb{Q}(\sqrt[3]{m}) \) denote the pure cubic number field that corresponds to \( \mathcal{H} \). Then the statements in the boxes below are all equivalent:

\[
\begin{align*}
p \text{ is represented by a form in } H & \quad \text{(1)} \quad \text{Dedekind} \quad p \text{ lies in the subgroup } \mathcal{H} \\
\text{p splits completely in } K(\sqrt[3]{m}) & \quad \text{(2)} \quad \text{Takagi} \\
p \equiv 1 \text{ mod } 3, \ (m/p)_{3} = 1 & \quad \text{(3)} \quad \text{Galois} \quad p \text{ splits completely in } \mathbb{Q}(\sqrt[3]{m}) \\
\end{align*}
\]

Here (1) is due to the isomorphism between class groups of forms and ray class groups, (2) is the decomposition law of class field theory together with the correspondence between class groups and class fields, and (3) uses the fact that we have assumed that \( p \equiv 1 \text{ mod } 3 \), and so \( p \) splits completely in \( K/\mathbb{Q} \). Finally, (4) is the decomposition law in Kummer extensions pulled down to \( \mathbb{Q}(\sqrt[3]{m}) \), which tells us that \( p \equiv 1 \text{ mod } 3 \) splits completely in this field if and only if \( (m/p)_{3} = 1 \).

The fact that \( p \) is represented by a form in \( H \) may also be formulated in a different way. It follows easily from Lagrange’s theory of equivalence that if a form with discriminant \( \Delta \) represents a prime number \( p \), then the form is equivalent to a form \( Q_p = (p,B,C) \) with first coefficient \( p \) and (of course) discriminant \( \Delta = B^2 - 4pc \).

The ring class groups modulo \( f \leq 20 \) whose order is divisible by 3, the structure of the ring class group, and the corresponding fields \( K = \mathbb{Q}(\sqrt[3]{m}) \) with disc \( K = -3f^2 \):

<table>
<thead>
<tr>
<th>( f )</th>
<th>( \text{Cl}(\Delta) )</th>
<th>( m )</th>
<th>( f )</th>
<th>( \text{Cl}(\Delta) )</th>
<th>( m )</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>([3])</td>
<td>2</td>
<td>15</td>
<td>([6])</td>
<td>5</td>
</tr>
<tr>
<td>9</td>
<td>([3])</td>
<td>3</td>
<td>17</td>
<td>([6])</td>
<td>17</td>
</tr>
<tr>
<td>10</td>
<td>([6])</td>
<td>10</td>
<td>18</td>
<td>([3,3])</td>
<td>6,12</td>
</tr>
<tr>
<td>12</td>
<td>([6])</td>
<td>( x )</td>
<td>19</td>
<td>([6])</td>
<td>19</td>
</tr>
<tr>
<td>14</td>
<td>([6])</td>
<td>28</td>
<td>20</td>
<td>([6,2])</td>
<td>( x )</td>
</tr>
</tbody>
</table>
In the two cases marked with an $x$, namely $f = 12$ and $f = 20$, the corresponding pure cubic fields come from $f = 6$ and $f = 10$, respectively; in these two cases, $f$ is a defining modulus for the class field, but not the conductor.

Thus we have finally proved Dedekind’s generalization of Euler’s conjectures using class field theory. This brings us to the next question: how did Dedekind prove this result? 20 years before class field theory became known?

The answer is that Dedekind proved his result by identifying a piece of the Dedekind zeta function of a pure cubic number field $K$ with what we would call an Artin zeta function of the abelian extension generated by $K$ over $\mathbb{Q}(\sqrt{-3})$, and that he did so by using the cubic reciprocity law.

**From ring classes to form classes.** For the proof of Dedekind’s theorem, all the correspondences between quadratic forms, ring class groups, class fields etc. must be explicit. In particular, we need a canonical isomorphism between the form class group $\text{Cl}(-3 \cdot f^2)$ and the ring class group modulo $f$ of $\mathbb{Q}(\sqrt{-3})$. This isomorphism will map ring classes to certain $\mathbb{Z}$-modules, which in turn are known to correspond to form classes by Dedekind’s supplements to Dirichlet’s lectures in number theory.

Since $k = \mathbb{Q}(\sqrt{-3})$ has class number 1, all ray classes are represented by the $\Phi(f)$ coprime residue classes modulo $f$. For $f \geq 3$, the six roots of unity in $k$ lie in different residue classes modulo $f$ and generate the same ray class, hence the number of ray classes is given by $\frac{1}{2} \Phi(f)$. The group structure on the ray classes is given by multiplication of principal ideals, i.e., $(\mu)(\nu) = (\mu \nu)$.

Two principal ideals $(\alpha)$ and $(\beta)$ coprime to $f$ generate the same ray class if $\alpha/\beta \equiv 1 \mod f$, and they generate the same ring class if $\alpha/\beta \equiv z \mod f$ for an integer $z$ coprime to $f$. The class $(\alpha)$ consists of elements of the form $\alpha z + \omega f$, where $z$ is an integer coprime to $f$ and $\omega$ an element of $\mathcal{O}_K$. Clearly $(\alpha)$ is not closed under addition, since $\alpha + \cdots + \alpha = f \alpha$ is not coprime to $f$. But we can consider the additive closure of $(\alpha)$, namely

$$k_\alpha = \alpha \mathbb{Z} + f \mathcal{O}.$$ 

This is a $\mathbb{Z}$-module of rank 2 in $\mathcal{O}$ containing $(\alpha)$, and these modules form a multiplicative group with respect to multiplication: the product of elements in $k_\alpha$ and $k_\beta$ is

$$(\alpha a + f \gamma)(\beta b + f \delta) = \alpha \beta \cdot ab + f(b \beta \gamma + a a \delta + f \gamma \delta) \in k_{\alpha \beta},$$

so we set $k_\alpha \cdot k_\beta = k_{\alpha \beta}$. This makes the modules $k_\alpha$ into a multiplicative group in such a way that the map $(\alpha) \mapsto k_\alpha$ induces an isomorphism from the ring class group modulo $f$ to the group of $\mathbb{Z}$-modules $k_\alpha$.

It is known that $\mathbb{Z}$-modules of rank 2 in $\mathcal{O}$ have a $\mathbb{Z}$-basis, i.e., given a module $k_\nu$ there exist elements $\alpha, \beta \in \mathcal{O}$ with $k_\nu = \alpha \mathbb{Z} + \beta \mathbb{Z}$.

**Lemma 10.1.** For such a basis we have $\alpha \beta' - \alpha' \beta = \pm \sqrt{-3} f$.

We choose the basis in such a way that the $+$ sign holds, and set

$$Q_\nu(x, y) = N(\alpha x + \beta y).$$

**Lemma 10.2.** $Q_\nu$ is a binary quadratic form with discriminant $-3f^2$. Changing the basis of the module changes the form by a unimodular transformation, and so leaves the class of $Q_\nu$ invariant.

Consider the ring class group modulo $f = 3k$ in $\mathbb{Q}(\sqrt{-3})$, where $k \equiv 2 \mod 9$ is squarefree. The classes $1, 1 + \sqrt{-3}k$ and $1 + 2\sqrt{-3}k$ form a subgroup of order 3 modulo $3k$. The module associated to $\nu = 1 + \sqrt{-3}k$ modulo $f$ is $k_\nu$. 

Lemma 10.3. We have \( k_\nu = \mathbb{Z} \oplus f\rho \mathbb{Z} = [1, f\rho] \) for \( \nu = 1 + \sqrt{-3} k \).

Thus the associated quadratic form is

\[
Q_\nu = N(x + f\rho y) = x^2 - fxy + f^2y^2
\]

with discriminant \(-3f^2\) as predicted.

In general we can always choose the first basis element as a natural number \( \alpha = m \); with \( \beta = t + n\rho \) we then have \( mn = f \), and the corresponding form is

\[
Q(x, y) = m^2x^2 + m(2t - n)xy + (t^2 - tn + n^2)y^2.
\]

Clearly \([\alpha, \beta] = [-\alpha, -\beta] = [\beta, -\alpha] = [-\beta, \alpha]\). Similarly, \([\alpha, \beta]\) and \(\rho[\alpha, \beta] = [\rho\alpha, \rho\beta]\) are equivalent because \(N(\rho) = 1\).

Lemma 10.4. Two such modules \( M \) and \( M_1 \) are equivalent if and only if \( M_1 = \rho M \) or \( M_1 = \rho^2 M \).

Consider the example \( f = 6 \). Let us first compute the ring class group modulo 6, which, in this case, happens to coincide with the full ray class group modulo 6. Since \( k = \mathbb{Q}(\sqrt{-3}) \) has class number 1, all ring classes are represented by residue classes modulo 6. Among the 36 residue classes, the number of residue classes coprime to 6 is \( \Phi(6) = 1 \). All ring classes are represented by the residue classes 1, \( 1 + 3\rho \), and 4 + 3\( \rho \) modulo 6. The group structure of these classes is determined by

\[
(1 + 3\rho)^2 = 1 + 6\rho + 9\rho^2 = 1 + 3(1 - \rho) \equiv 4 + 3\rho \mod 6.
\]

The modules \([m, t + n\rho]\) satisfying \( mn = 6 \) and \( 0 \leq t < m \) are

- \( m = 1 \): \([1, 6\rho]\)
- \( m = 2 \): \([2, 3\rho], [2, 1 + 3\rho]\)
- \( m = 3 \): \([3, 2\rho], [3, 1 + 2\rho], [3, 2 + 2\rho]\)
- \( m = 6 \): \([6, \rho], [6, 1 + \rho], [6, 2 + \rho], [6, 3 + \rho], [6, 4 + \rho], [6, 5 + \rho]\)

Since \(N(1 + 2\rho) = 3\), the module \([3, 1 + 2\rho]\) must be excluded. The same goes for \([6, 2 + \rho]\) and \([6, 5 + \rho]\).

The remaining 9 modules come in triples of equivalent forms:

- \([1, 6\rho] \sim [6, \rho] \sim [6, 1 + \rho]\);
- \([2, 3\rho] \sim [3, 2 + 2\rho] \sim [6, 3 + \rho]\);
- \([2, 1 + 3\rho] \sim [3, 2\rho] \sim [6, 4 + \rho]\).

In fact we have

- \(\rho[1, 6\rho] = \rho[6, \rho^2] = [\rho, -6 - 6\rho] = [6 + 6\rho, \rho] = [6, \rho]\)
- \(\rho^2[1, 6\rho] = \rho^2[6, \rho] = [-1 - \rho, 6] = [6, 1 + \rho]\),

Thus we have the following 3 modules:

<table>
<thead>
<tr>
<th>ring class</th>
<th>module</th>
<th>form</th>
<th>reduced form</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>[1, 6\rho]</td>
<td>(1, -6, 36)</td>
<td>(1, 0, 27)</td>
</tr>
<tr>
<td>(1 + 3\rho)</td>
<td>[2, 1 + 3\rho]</td>
<td>(4, -2, 7)</td>
<td>(4, -2, 7)</td>
</tr>
<tr>
<td>(4 + 3\rho)</td>
<td>[2, 3\rho]</td>
<td>(4, -6, 9)</td>
<td>(4, 2, 7)</td>
</tr>
</tbody>
</table>
Note that \(1 + 3\rho \in [2, 1 + 3\rho]\) and \(-2 + 3\rho \in [2, 3\rho]\).

In order to do these calculations in general, we need a set of representatives for the generators of the ring class group modulo \(f\), i.e., a system of representatives for the cosets \((\mathcal{O}/f)^\times/(-\rho)\). Let us consider the special case \(f = 3p\) for some prime \(p \equiv 2, 5 \mod 9\). If we use the integral basis \(\{1, \omega\}\) with \(\omega = 1 + \rho\), then \(a + b\rho\) is divisible by \(\omega\) if and only if \(3 \mid a\), and divisible by \(p\) if and only if \(p \mid a\) and \(p \mid b\). Thus a complete system of coprime residue classes modulo \(f\) is given by the elements \(a + b\omega\) with \(0 \leq a, b \leq f - 1\), with the following elements omitted:

- The elements divisible by \(\sqrt{-3}\), namely \(b\omega, 3 + b\omega, 6 + b\omega, \ldots, f - 3 + b\omega\) with \(0 \leq b \leq f - 1\). There are \(3p^2\) such elements.
- The elements divisible by \(p\) and not by \(\sqrt{-3}\), namely \(p\omega, 2p\omega, p + p\omega, p + 2p\omega, 2p + p\omega, 2p + 2p\omega\). There are 6 such elements.

This agrees with the fact that there are \(\Phi(3p) = 6(p^2 - 1)\) coprime residue classes.

better idea: start with forms!

If \(f = 3p\), then we start with the group \(\text{Cl}(-3 \cdot 3^2)\); its element is represented by the form \(Q_0 = (1, 1, 7)\). The number of elements in \(\text{Cl}(-3 \cdot f^2)\) is \(p + 1\). The form \(Q_a = (a^2 + a + 7, 2a + 1, 1)\) has discriminant \(-27\) and represents \(1\), hence is equivalent to \(Q_0\). Now we produce the derived forms \(Q_a^* = (a^2 + a + 7, (2a + 1)p, p^3)\) for \(a = 0, 1, \ldots, p - 1\) and \(Q_\infty = (7p^2, p, 1)\).

\(p = 2, f = 6:\) the forms are

\[
Q_0^* = (7, 2, 4), \quad Q_1^* = (9, 6, 4), \quad Q_\infty = (28, 2, 1).
\]

\(p = 5, f = 15:\)

\[
\begin{array}{c|cccc|cc}
 a & Q_a & \text{reduced} & \text{module} \\
\hline
\infty & (175, 5, 1) & (1, 1, 169) & [1, 15\rho] \\
0 & (7, 5, 25) & (7, 5, 25) & [5, 1 + 3\rho] \\
1 & (9, 15, 25) & (9, -3, 19) & [5, 3\rho] \\
2 & (13, 25, 25) & (13, 1, 13) & [5, -1 + 3\rho] \\
3 & (19, 35, 25) & (9, 3, 19) & [5, -2 + 3\rho] \\
4 & (27, 45, 25) & (7, -5, 25) & [5, -3 + 3\rho] \\
\end{array}
\]

\[
\begin{array}{cccccc}
\infty & \infty & 0 & 1 & 2 & 3 & 4 \\
0 & 0 & 1 & 2 & 3 & 4 \\
1 & 1 & 4 & 3 & 0 & \infty & 2 \\
2 & 2 & 1 & 0 & \infty & 4 & 3 \\
3 & 3 & 2 & \infty & 4 & 1 & 0 \\
4 & 4 & \infty & 2 & 3 & 0 & 1 \\
\end{array}
\]

It can be verified that the group law induced by composition is given by

\[
[Q_r] * [Q_s] = [Q_t] \quad \text{with} \quad t \equiv \frac{rs - 2}{r + s + 1} \mod 5.
\]

Start with modules!
We have

\[\text{Proof.}\]

\[\text{Assume that } p \nmid a \text{ integers if } 3 \nmid a.\]

Write \( a \equiv p \mod (1 + 3p) \), hence \( a \equiv p \mod (1 + 3p) \), i.e., \( a \equiv p \mod (1 + 3p) \), and have used the fact that \( 3B - aC \) represents all integers if \( 3 \nmid a.\)

\[\text{Lemma 10.5. Assume that } f = 3p \text{ for } p \equiv 2, 5 \mod 9. \text{ If } 3 \nmid a, \text{ then } (a + 3p)\mathbb{Z} + f\mathcal{O} = [p, a + 3p].\]

\[\text{Proof.}\]

\[\text{We have}\]

\[(a + 3p)\mathbb{Z} + f\mathcal{O} = \{aA + 3Ap + 3pB + 3pCp\} = \{aA + 3pB + 3(A + pC)p\}\]

\[= \{a(D - pC) + 3pB + 3Dp\} = \{p(3B - aC) + D(a + 3p)\}\]

\[= p\mathbb{Z} + (a + 3p)\mathbb{Z},\]

where we have introduced \( A = D - pC, \) and have used the fact that \( 3B - aC \) represents all integers if \( 3 \nmid a.\)

\[\text{One more for the road. Assume that } p = a^2 + 3ab + 9b^2, \text{ and let } q \text{ be a prime number } \neq p.\]

Write \( a \equiv 3kb \mod q, \) i.e., \( a = 3kb + qx; \) then

\[p = a^2 + 3ab + 9b^2 = q^2 x^2 + (6k + 1)bqx + b^2(1 + 3k + 9k^2),\]

hence \( p \) is represented by the form \( Q_k = (q^2, (6k + 1)q, 1 + 3k + 9k^2) \) with discriminant \(-3q^2.\)

Or: assume that \( p = a^2 + 3b^2, \) and let \( q \) be a prime number \( \neq p. \) Write \( a \equiv kb \mod q, \)

i.e., \( a = kb + qx; \) then

\[p = a^2 + 3b^2 = q^2 x^2 + 2bkqx + b^2(k^2 + 3),\]

hence \( p \) is represented by \( Q_k = (q^2, 2kq, k^2 + 3) \) with discriminant \( \Delta = -12q^2.\)

Composition law?
11. QUARTIC RECIPROCITY

Although Dedekind only discussed the cubic case, he knew that biquadratic residues may be treated in an analogous way. Here we will briefly review the relevant details.

**Pure quartic extensions.**

12. DEDEKIND ZETA FUNCTIONS AND L-SERIES

Following Dirichlet and Kummer, who used $L$-series attached to cyclotomic number fields, Dedekind defined the zeta function $\zeta_K(s)$ of a number field $K$ by

$$\zeta_K(s) = \sum \frac{1}{N(a)^s},$$

where the sum is over all integral nonzero ideals $a$. Unique factorization into prime ideals shows that the Dedekind zeta function admits an Euler factorization

$$\zeta_K(s) = \prod \frac{1}{1 - \frac{1}{N(p)^s}},$$

where the product is over all prime ideals $p$ in $K$. Both the sum and the product converge absolutely in the half plane $\text{Re } s > 1$.

**L-series of genus class fields.** The genus class field of the quadratic number field $K$ with discriminant $\Delta$ is the multiquadratic extension

$$K_{\text{gen}} = \mathbb{Q}(\sqrt{\Delta_1}, \ldots, \sqrt{\Delta_t}),$$

where $\Delta = \Delta_1 \cdots \Delta_t$ is the factorization of $\Delta$ into prime discriminants. Since inertia groups are cyclic, each prime $p \mid \Delta$ either splits into $2^t = (K_{\text{gen}} : \mathbb{Q})$ prime ideals of degree 1 or into $2^{t-1}$ prime ideals of degree 2.

If $p$ splits completely, then the product of all Euler factors attached to the prime ideals above $p$ is

$$\left(\frac{1}{1 - p^{-s}}\right)^{2^t}.$$

If $p$ does not split completely, the product of the corresponding Euler factors is

$$\left(\frac{1}{1 - p^{-2s}}\right)^{2^{t-1}} = \left(\frac{1}{1 - p^{-s}}\right)^{2^{t-1}} \left(\frac{1}{1 + p^{-s}}\right)^{2^{t-1}}.$$

**L-series of $\mathbb{Q}(i, \sqrt{5})$.** Consider the number field $K = \mathbb{Q}(i, \sqrt{5})$; we will determine the Euler factorization of the Dedekind zeta function $\zeta_K(s)$ by looking at the prime ideal decomposition in $K$. Let $F_p(s)$ denote the product of all Euler factors at the prime ideals above $p$.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$pO_K$</th>
<th>$F_p(s)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$p^2$</td>
<td>$(1 - p^{-2s})^{-1}$</td>
</tr>
<tr>
<td>5</td>
<td>$p_1^2p_2^2$</td>
<td>$(1 - p^{-s})^{-2}$</td>
</tr>
<tr>
<td>$p \equiv 1, 9 \mod 20$</td>
<td>$p_1p_2p_3p_4$</td>
<td>$(1 - p^{-s})^{-4}$</td>
</tr>
<tr>
<td>$p \equiv 3, 7 \mod 20$</td>
<td>$p_1p_2$</td>
<td>$(1 - p^{-2s})^{-2}$</td>
</tr>
<tr>
<td>$p \equiv 11, 19 \mod 20$</td>
<td>$p_1p_2$</td>
<td>$(1 - p^{-2s})^{-2}$</td>
</tr>
<tr>
<td>$p \equiv 13, 17 \mod 20$</td>
<td>$p_1p_2$</td>
<td>$(1 - p^{-2s})^{-2}$</td>
</tr>
</tbody>
</table>
If we define the characters \( \chi_1(p) = \left( \frac{-1}{p} \right) \), \( \chi_2(p) = \left( \frac{2}{p} \right) \) and \( \chi_3(p) = \left( \frac{-5}{p} \right) \), then we can write the Euler factor in each case as
\[
F_p(s) = (1 - p^{-s})^{-1}(1 - \chi_1(p)p^{-s})^{-1}(1 - \chi_2(p)p^{-s})^{-1}(1 - \chi_3(p)p^{-s})^{-1}.
\]
This shows immediately that
\[
\zeta_K(s) = \zeta(s)L(s, \chi_1)L(s, \chi_2)L(s, \chi_3).
\]
If we denote the quadratic subfields by \( k_1 = \mathbb{Q}(\sqrt{1}) \), \( k_2 = \mathbb{Q}(\sqrt{5}) \) and \( k_3 = \mathbb{Q}(\sqrt{-5}) \), and the zeta function of \( k_j \) by \( \zeta_j(s) \), then we have
\[
\zeta_j(s) = \zeta(s)L(s, \chi_j).
\]
This implies that
\[
\frac{\zeta_K(s)}{\zeta(s)} = \frac{\zeta_1(s)}{\zeta(s)} \cdot \frac{\zeta_2(s)}{\zeta(s)} \cdot \frac{\zeta_3(s)}{\zeta(s)} = L(s, \chi_2)L(s, \chi_3).
\]
This in turn shows that
\[
\frac{\zeta_K(s)}{\zeta_1(s)} = \frac{\zeta_2(s)}{\zeta(s)} \cdot \frac{\zeta_3(s)}{\zeta(s)} = L(s, \chi_2)L(s, \chi_3).
\]
Next we consider \( K \) as a quadratic unramified extension of \( k_3 = \mathbb{Q}(\sqrt{-5}) \). Since \( k_3 \) has class number 2, the ideal class group \( \text{Cl}(k_3) \) has two characters, the trivial character \( \chi \) and the character \( \psi \), which takes the value \(-1\) on nonprincipal ideals. The two \( L \)-series attached to \( \text{Cl}(k_3) \) thus are
\[
L(s, \chi) = \prod_p \left( 1 - \frac{1}{Np^s} \right) \quad \text{and} \quad L(s, \psi) = \prod_p \left( 1 - \frac{\psi(p)}{Np^s} \right).
\]
Let us first look at \( L(s, \chi) = \zeta_3(s) \) and its Euler factors \( F_{p, \chi}(s) \):
\[
\begin{array}{c|cc}
 p & p\mathcal{O}_3 & F_{p, \chi}(s) \\
 \hline
 2 & p^2 & (1 - p^{-s})^{-1} \\
 5 & p^2 & (1 - p^{-s})^{-1} \\
 (-5/p) = +1 & p_1p_2 & (1 - p^{-s})^{-2} \\
 (-5/p) = -1 & (p) & (1 - p^{-2s})^{-1}
\end{array}
\]
For the character \( \psi \) we find the following table, where \( F_1(s) \) denotes the Euler factors at \( p \) of \( L(s, \chi_1) \), and \( F_2(s) \) those of \( L(s, \chi_2) \):
\[
\begin{array}{c|cc|cc}
 p & p\mathcal{O}_3 & F_{p, \chi}(s) & F_1(s) & F_2(s) \\
 \hline
 2 & p^2 & (1 + p^{-s})^{-1} & 1 & (1 - p^{-s})^{-1} \\
 5 & p^2 & (1 - p^{-s})^{-1} & (1 - p^{-s})^{-1} & 1 \\
 (-1/p) = (5/p) = +1 & p_1p_2 & (1 - p^{-s})^{-2} & (1 - p^{-s})^{-1} & (1 - p^{-s})^{-1} \\
 (-1/p) = (5/p) = -1 & p_1p_2 & (1 + p^{-s})^{-2} & (1 + p^{-s})^{-1} & (1 + p^{-s})^{-1} \\
 (-1/p) = -1, (5/p) = +1 & (p) & (1 - p^{-2s})^{-1} & (1 + p^{-s})^{-1} & (1 - p^{-s})^{-1} \\
 (-1/p) = +1, (5/p) = -1 & (p) & (1 + p^{-2s})^{-1} & (1 - p^{-s})^{-1} & (1 + p^{-s})^{-1}
\end{array}
\]
This shows that we have
\[
L(s, \psi) = L(s, \chi_1)L(s, \chi_2).
\]
General biquadratic extensions. Let $K/k$ be a biquadratic extension with quadratic subextensions $k_1/k$, $k_2/k$ and $k_3/k$. For each prime ideal $p$ in $k$ there are the following possibilities.

<table>
<thead>
<tr>
<th>$K_Z$</th>
<th>$K_T$</th>
<th>$pO_K$</th>
<th>$F_e(p)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K$</td>
<td>$K$</td>
<td>$\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4$</td>
<td>$(1 - Np^{-s})^{-4}$</td>
</tr>
<tr>
<td>$k_j$</td>
<td>$K$</td>
<td>$\mathfrak{P}_1\mathfrak{P}_2$</td>
<td>$(1 - Np^{-2s})^{-2}$</td>
</tr>
<tr>
<td>$k_j$</td>
<td>$k_j$</td>
<td>$\mathfrak{P}_1^7\mathfrak{P}_2^2$</td>
<td>$(1 - Np^{-s})^{-2}$</td>
</tr>
<tr>
<td>$k$</td>
<td>$k$</td>
<td>$\mathfrak{P}_4$</td>
<td>$(1 - Np^{-s})^{-1}$</td>
</tr>
</tbody>
</table>

Define quadratic characters $\chi_j$ by $\chi_j(p) = +1$ or $-1$ according as $p$ splits or is inert in $k_j$. Thus

$$\zeta_K(s) = \zeta_k(s)L(s, \chi_1)L(s, \chi_2)L(s, \chi_3).$$

An example with cyclic class group of order 4. Now consider the quadratic number field with discriminant $\Delta = -55$. Its class group is cyclic of order 4, and the form class group is generated by $Q_1 = (2, 1, 7)$, and its powers are $Q_1^2 \sim (4, 3, 4), Q_1^3 \sim (2, -1, 7)$ and $Q_1^4 \sim Q_0 = (1, 1, 14)$. Genus theory provides us with the following result concerning the representation of primes:

<table>
<thead>
<tr>
<th>condition</th>
<th>represented by</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(5/p) = (-11/p) = +1$</td>
<td>$(1, 1, 14), (4, 3, 4)$</td>
</tr>
<tr>
<td>$(5/p) = (-11/p) = -1$</td>
<td>$(2, \pm 1, 7)$</td>
</tr>
</tbody>
</table>

The Hilbert class field of $K = \mathbb{Q}(\sqrt{-55})$ is given by

$$K^1 = K\left(\sqrt{3 + 2\sqrt{5}}\right) = K^1\left(\sqrt{-1 + 2\sqrt{-11}}\right) = K\left(\sqrt{3+\sqrt{-11}}/2\right).$$

We now study the Euler factorization of the $L$-series of $K^1/\mathbb{Q}$. For primes $p \nmid \Delta$ with $(5/p) = (-11/p) = +1$ we write $\alpha = 3 + 2\sqrt{5}$ and $\beta = -1 + 2\sqrt{-11}$ and set $(\alpha/p) = 1$ if $p$ splits completely in $K^1$. We let $K_Z$ denote the decomposition field of $p$, and $(e, f, g)$ the vector giving the ramification index $e$, the inertia degree $f$ and the number of primes above $p$ in $K^1$. Finally, set $F_1 = \mathbb{Q}(\sqrt{5}, \sqrt{\alpha})$ and $F_2 = \mathbb{Q}(\sqrt{-11}, \sqrt{\beta})$.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$K_Z$</th>
<th>$(f, g)$</th>
<th>$F_p(s)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(5/p) = (-11/p) = +1, (\alpha/p) = +1$</td>
<td>$K^1$</td>
<td>$(1, 8)$</td>
<td>$(1 - p^{-s})^{-8}$</td>
</tr>
<tr>
<td>$(5/p) = (-11/p) = +1, (\alpha/p) = -1$</td>
<td>$K_{gen}$</td>
<td>$(2, 4)$</td>
<td>$(1 - p^{-2s})^{-4}$</td>
</tr>
<tr>
<td>$(5/p) = (-11/p) = -1$</td>
<td>$K$</td>
<td>$(4, 2)$</td>
<td>$(1 - p^{-4s})^2$</td>
</tr>
<tr>
<td>$(5/p) = +1, (-11/p) = -1, (\alpha/p) = +1$</td>
<td>$F_1$</td>
<td>$(2, 4)$</td>
<td>$(1 - p^{-2s})^{-4}$</td>
</tr>
<tr>
<td>$(5/p) = -1, (-11/p) = +1, (\beta/p) = +1$</td>
<td>$F_2$</td>
<td>$(2, 4)$</td>
<td>$(1 - p^{-2s})^{-4}$</td>
</tr>
</tbody>
</table>

The genus field $L = K_{gen}$ has class number 2, hence there are two characters of the class group, the trivial character $\chi$ and the character $\psi$ of order 2. We have

$$\zeta_{K^1}(s) = L(s, \chi)L(s, \psi), \quad \text{where } L(s, \chi) = \zeta_L(s).$$

We have already seen that

$$\zeta_L(s) = \zeta(s)L(s, \chi_1)L(s, \chi_2)L(s, \chi_3).$$
where \( \chi_j \) are the Dirichlet characters associated to the quadratic subfields of \( L \). For the nontrivial character \( \psi \) of the class group \( \text{Cl}(L) \) we find the following table. Here \( p \) is a prime ideal above \( p \) in \( L \), and \( p \) is represented by the form \( Q \).

<table>
<thead>
<tr>
<th>( p )</th>
<th>( Q )</th>
<th>( \psi(p) )</th>
<th>( F_p(s) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( (5/p) = (-11/p) = +1 )</td>
<td>(1, 1, 14)</td>
<td>+1</td>
<td>((1 - p^{-s})^4)</td>
</tr>
<tr>
<td>( (5/p) = (-11/p) = +1 )</td>
<td>(4, 3, 4)</td>
<td>-1</td>
<td>((1 + p^{-s})^4)</td>
</tr>
<tr>
<td>( (5/p) = (-11/p) = -1 )</td>
<td>(2, ±1, 7)</td>
<td>-1</td>
<td>((1 + p^{-2s})^2)</td>
</tr>
<tr>
<td>( (5/p) = +(-11/p) )</td>
<td>-</td>
<td>+1</td>
<td>((1 - p^{-2s})^2)</td>
</tr>
</tbody>
</table>

Finally let us look at the unramified cyclic quartic extension \( K^1/k_3 \). There are four characters of the class group, namely the powers of the character \( \psi \) defined by \( \psi([p]) = i \), where \( p = (7, 1 + \sqrt{-55}) \) is the prime ideal above \( 7 \) generating the class group of \( k_3 \). As above, the trivial character \( \chi \) gives rise to the \( L \)-series \( L(s, \chi) = \zeta(s) \zeta(s)L(s, \chi_3) \). Observe that \( \psi(q) = i \) for the prime ideals \( q \in [p] \), where \( q = Nq \) satisfies \( (5/q) = (-11/q) = -1 \).

<table>
<thead>
<tr>
<th>( q )</th>
<th>( \psi(q) )</th>
<th>( F_q(s) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( (5/q) = (-11/q) = -1 )</td>
<td>±i</td>
<td>((1 - iq^{-s})^{-1}(1 + iq^{-s})^{-1})</td>
</tr>
<tr>
<td>( (5/q) = (-11/q) = +1, (\alpha/p) = -1 )</td>
<td>-1</td>
<td>((1 + q^{-s})^{-2})</td>
</tr>
<tr>
<td>( (5/q) = (-11/q) = +1, (\alpha/p) = +1 )</td>
<td>+1</td>
<td>((1 - q^{-s})^{-2})</td>
</tr>
<tr>
<td>( (5/q) = +(-11/q) )</td>
<td>+1</td>
<td>((1 - q^{-2s})^{-1})</td>
</tr>
</tbody>
</table>

Finally, the relevant information concerning \( L(s, \psi^2) \) is given by the following table.

<table>
<thead>
<tr>
<th>( q )</th>
<th>( \psi^2(q) )</th>
<th>( F_q(s) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>+1</td>
<td>((1 - 5^{-s})^{-1})</td>
</tr>
<tr>
<td>11</td>
<td>+1</td>
<td>((1 - 11^{-s})^{-1})</td>
</tr>
<tr>
<td>( (5/q) = (-11/q) = -1 )</td>
<td>-1</td>
<td>((1 + q^{-s})^{-2})</td>
</tr>
<tr>
<td>( (5/q) = (-11/q) = +1 )</td>
<td>+1</td>
<td>((1 - q^{-s})^{-2})</td>
</tr>
<tr>
<td>( (5/q) = -(-11/q) )</td>
<td>+1</td>
<td>((1 - q^{-2s})^{-1})</td>
</tr>
</tbody>
</table>

**L-series of pure cubic fields.** It follows quickly from the general analytic class number formula proved by Dedekind that in the case of pure cubic number fields \( K = \mathbb{Q}(\sqrt[3]{m}) \) we have

\[
\lim_{s \to 1} (s - 1) \zeta_K(s) = h \cdot \frac{2\pi \log \varepsilon}{\sqrt{|D|}},
\]

where \( \varepsilon > 1 \) is the fundamental unit of \( K \) and where we may write \( \sqrt{|D|} = k\sqrt{3} \).

Let \( L = \mathbb{Q}(\sqrt[3]{m}, \sqrt{-3}) \) denote the normal closure of \( K \). Then we can attach zeta functions to the subfields of \( L/\mathbb{Q} \), namely

- the Riemann zeta function \( \zeta(s) \) to the base field \( \mathbb{Q} \);
- the zeta function \( \zeta_k(s) \) to the subfield \( k = \mathbb{Q}(\sqrt{-3}) \);
- the zeta function \( \zeta_K(s) \) to the subfield \( K = \mathbb{Q}(\sqrt[3]{m}) \) (and its conjugates);
the zeta function $\zeta_L(s)$.

For finding relations between these zeta functions we look at their Euler factors.

$\zeta_k(s)$. The prime number $p$ splits in $k$ if and only if $\left( \frac{-3}{p} \right) = +1$. In this case, there are two prime ideals $p$ and $p'$ over $p$, and the associated Euler factors are

\[ F_p(s) = \left( \frac{1}{1 - p^{-s}} \right) \cdot \left( \frac{1}{1 - p^{-s}} \right). \]

If $\left( \frac{-3}{p} \right) = +1$, then $p$ is inert, and we have the Euler factor

\[ F_p(s) = \frac{1}{1 - p^{-2s}} = \left( \frac{1}{1 - p^{-s}} \right) \cdot \left( \frac{1}{1 + p^{-s}} \right). \]

Thus in both cases the product of the Euler factors of the prime ideals above $p$ is given by

\[ F_p(s) = \left( \frac{1}{1 - p^{-s}} \right) \cdot \left( \frac{1}{1 - \chi(p)p^{-s}} \right), \]

where $\chi(p) = (\Delta/p)$. This implies that

\[ \zeta_k(s) = \zeta(s)L(s, \chi), \]

where $L(s, \chi) = \prod \frac{1}{1 - \chi(p)p^{-s}}$ is the Dirichlet $L$-series attached to the character $\chi$.

$\zeta_K(s)$. By the decomposition law in pure cubic number fields there are the following possibilities for a prime number $p \nmid \Delta$:

1. $p \equiv 1 \mod 3$ splits completely. Then

\[ F_p(s) = \left( \frac{1}{1 - p^{-2s}} \right)^3. \]

2. $p \equiv 1 \mod 3$ is inert. Then

\[ F_p(s) = \left( \frac{1}{1 - p^{-3s}} \right) = \left( \frac{1}{1 - p^{-s}} \right) \cdot \left( \frac{1}{1 + p^{-s} + p^{-2s}} \right) = \left( \frac{1}{1 - p^{-s}} \right) \cdot \left( \frac{1}{1 - \rho p^{-s}} \right) \cdot \left( \frac{1}{1 - \rho^2 p^{-s}} \right), \]

where $\rho$ is a primitive cube root of unity.

3. $p \equiv 2 \mod 3$ splits into two prime ideals. In this case,

\[ F_p(s) = \left( \frac{1}{1 - p^{-s}} \right) \left( \frac{1}{1 - p^{-2s}} \right). \]

$\zeta_L(s)$. The extension $L/Q$ is normal and noncyclic. Since inertia subgroups are cyclic, no prime can be inert in $L$. Thus we are left with the following possibilities for primes $p \nmid \text{disc } L$.

1. $p$ splits completely, i.e., $p \equiv 1 \mod 3$ and $(m/p)_3 = 1$. In this case

\[ F_p(s) = \left( \frac{1}{1 - p^{-s}} \right)^6. \]

2. $p$ has inertia degree 2, i.e., $p \equiv 2 \mod 3$. Then

\[ F_p(s) = \left( \frac{1}{1 - p^{-2s}} \right)^3 = \left( \frac{1}{1 - p^{-s}} \right)^3 \left( \frac{1}{1 + p^{-s}} \right)^3. \]
(3) $p$ has inertia degree 3, i.e., $p \equiv 1 \mod 3$ and $(m/p)_3 \neq 1$. Then
\[ F_p(s) = \left( \frac{1}{1 - p^{-3s}} \right)^2 = \left( \frac{1}{1 - p^{-s}} \right)^2 \left( \frac{1}{1 - \rho p^{-s}} \right)^2 \left( \frac{1}{1 - \rho^2 p^{-s}} \right)^2. \]

If we combine our results so far we find that
\[ \zeta_L(s) \zeta(s) = \zeta_K(s) \zeta(s) \cdot \left( \frac{\zeta_K(s)}{\zeta(s)} \right)^2. \]

We leave the verification that this identity also holds for the Euler factors of the ramified primes as an exercise.

Taking the limit $s \to 1$ of this identity and using the evaluation of the residue of Dedekind’s zeta function at $s = 1$ yields a class number formula of the form
\[ h_L = c(K) h_K^2 \]
for a small constant $c(K)$ that depends essentially on the index of the group generated by the units of the proper subfields of $L$ inside the unit group of $L$. Such questions were later taken up again by Arnold Scholz.

13. Artin L-series

As in the last section, we will omit the discussion of the ramified primes. For abelian extensions $L/K$, Hecke had shown that the zeta function of $L$ can be factored into a product of $L$-series for certain generalizations of Dirichlet characters. In his attempts to do something similar for nonabelian extensions, Artin had to take even more general characters into account, namely characters coming from representations of finite groups.

Assume therefore that $L/K$ is a normal extension with Galois group $G$, and let $(V, \rho)$ be a representation of $G$. This means that $V$ is a complex vector space, and $\rho: G \to \text{GL}(V)$ is a group homomorphism that sends an element of the Galois group to an invertible linear map $V \to V$. If $V$ has dimension $n$ we can think of $\text{GL}(V)$ as the group of $n \times n$-matrices with entries from $\mathbb{C}$.

Given a representation $\rho$ of the Galois group of a normal extension $L/K$, we can define an associated Artin $L$-series by
\[ L(s, \rho) = \prod_p \det(I - Np^{-s} \rho(\phi_p))^{-1}, \]
where the product is over all (unramified) prime ideals $p$ in $K$ and $\mathfrak{P}$ is an arbitrary prime ideal in $L$ above $p$. The readers should bear in mind that this definition is incomplete in that the Euler factors at the ramified primes have to be taken into consideration as well. We should also observe that picking a different prime ideal $\mathfrak{P}$ above $p$ amounts to replacing the Frobenius automorphism by one of its conjugates, and this does not change the determinant.

If $L/K$ is an abelian extension, something special happens. On the one hand, class field theory predicts that, in this case,
\[ \zeta_L(s) = \prod L(s, \chi) \]
is a product of $L$-series, where $\chi$ runs through the $(L: K)$ characters of the ray class group $\text{Cl}(m)$ associated to the class field $L$. For the trivial character $\chi_1$, we have $L(s, \chi_1) = \zeta_K(s)$. On the other hand, there are $(L: K)$ irreducible representations $\rho$ of the abelian Galois group $G = \text{Gal}(L/K)$. Artin conjectured that these $L$-series are just the $L$-series for the characters of the ray class group. This identification between the classical $L$-series and those of Artin would follow easily from the following theorem, which Artin called the general reciprocity law:
Theorem 13.1 (Artin’s reciprocity law). Let \( L \) be the class field for the ray class group \( \operatorname{Cl}(m) \) in \( K \). The Frobenius automorphism \( \phi_p \) of a prime ideal \( p \mid m \) only depends on the class of \( p \) in \( \operatorname{Cl}(m) \), and the map \( p \mapsto \phi_p \) induces an isomorphism

\[
\operatorname{Art} : \operatorname{Cl}(m) \longrightarrow \operatorname{Gal}(L/K).
\]

Quadratic Extensions. As a baby-example consider quadratic extensions \( L = \mathbb{Q}(\sqrt{m}) \) with discriminant \( \Delta \) and Galois group \( G = \{1, \sigma\} \). In order to make the transition to the case of cubic extensions easier, let us write \( \alpha = \sqrt{m} \) and \( \beta = -\sqrt{m} \). The automorphisms of \( L/\mathbb{Q} \) either fix these elements or swap them. In particular, for every \( \sigma \in G \) there is a \( 2 \times 2 \)-matrix \( M(\sigma) \) satisfying \( (\beta) \sigma = M(\sigma)(\beta) \), and in fact we have

\[
M(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad M(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.
\]

This is a 2-dimensional representation of \( G \) since

\[
M(\sigma \tau) = (\beta) \sigma \tau = M(\sigma)(\beta) \tau = M(\sigma)M(\tau).
\]

Now let \( p \mid \Delta \) be a prime number and \( p \) a prime above \( p \) in \( L \). The Frobenius automorphism \( \phi_p \) of \( p \) is an element of \( G \), and so \( \rho(\phi_p) \) is a \( 2 \times 2 \)-matrix, to which we can associate the polynomial \( g(p) = \det(I - Np^{-s} \cdot \rho(\phi_p)) \) in \( \frac{1}{p} \). The statement that the Frobenius automorphism of a prime ideal \( p \) only depends on the ray class generated by \( p \) is known as Artin’s reciprocity law. Now we find

\[
\begin{array}{c|ccc}
p & \phi_p & \rho(\phi_p) & g(p) \\
\hline
p \in \mathcal{H} & 1 & (\frac{1}{1} \frac{0}{1}) & (1 - p^{-s})^{-2} \\
p \notin \mathcal{H} & \sigma & (\frac{0}{1} \frac{1}{0}) & (1 - p^{-2s})^{-1}
\end{array}
\]

These factors look a lot like the Euler factors of the Dedekind zeta function of \( K \). We will now have a closer look at the factors coming from Artin’s construction.

To this end, consider the group \( D \) of coprime residue classes modulo 20. The residue classes 1, 3, 7 and 9 modulo 20 form a subgroup \( H \) of index 2 in \( D \), and \( L \) is the corresponding class field. Thus the primes \( p \) whose residue classes modulo 20 lie in \( H \) are the primes that split in \( L \), and the other primes remain inert (we do not consider ramified primes).

Now the product of the Euler factors at \( p \) in Artin’s \( L \)-funtion above is \((1 - p^{-s})^{-2} \) for primes \( p \equiv 1, 3, 7, 9 \) mod 20, whereas in Dedekind’s zeta function we have this Euler factor for primes \( p \) with \( (\Delta) = +1 \). Thus Artin’s \( L \)-function will coincide with Dedekind’s if

\[
(\Delta) = +1 \quad \text{if and only if} \quad p \equiv 1, 3, 7, 9 \text{ mod } 20.
\]

In other words: the claim that the Euler factors of Artin’s \( L \)-series and of Dedekind’s zeta function coincide is equivalent to the quadratic reciprocity law for the symbol \( (\Delta) \).

Pure Cubic Extensions. Let us now look at the situation in the normal extensions \( L = \mathbb{Q}(\sqrt{-3}, \sqrt{m}) \), where we will follow the presentation given by Stark [26]. Here \( L \) is abelian over the subfield \( k = \mathbb{Q}(\sqrt{-3}) \). Let \( G = \operatorname{Gal}(L/\mathbb{Q}) \) be the Galois group of \( L/\mathbb{Q} \). The Galois group permutes the roots \( \alpha = \sqrt{m} \), \( \beta = \rho \alpha \) and \( \gamma = \rho^2 \alpha \). The cyclic permutation \( (\alpha \beta \gamma) \) has order 3, and the three permutations \( (\alpha \beta), (\alpha \gamma) \) and \( (\beta \gamma) \) have order 3. To each \( \sigma \in G \) we can attach a \( 3 \times 3 \)-matrix \( M(\sigma) \) by demanding that

\[
(\begin{smallmatrix} \alpha & \beta \\ \beta & \gamma \end{smallmatrix}) \sigma = M(\sigma)(\begin{smallmatrix} \alpha & \beta \\ \beta & \gamma \end{smallmatrix}).
\]
This gives rise to the following “permutation” representation of \( G \) defined by

\[
\begin{align*}
D(1) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & D(\alpha\beta\gamma) &= \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} & D(\alpha\gamma) &= \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \\
D(\alpha\beta) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & D(\alpha\gamma) &= \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} & D(\beta) &= \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}
\end{align*}
\]

Next we look at the Euler factors of Artin’s L-function attached to this representation \( \rho : \sigma \mapsto M(\sigma) \). In the following table, the pair \((f,g)\) denotes the inertia degree and the number of prime ideals \( \Psi \) above \( p \) in \( L \):

\[
\begin{array}{c|ccc}
p & (f,g) & \phi_p & \det(I - Np^{-s}\rho(\phi_p))^{-1} \\
p \in \mathcal{H} & (1,6) & 1 & (1 - p^{-s})^{-3} \\
p \cdot \mathcal{H} \text{ has order 3} & (3,2) & (\alpha\beta\gamma) & (1 - p^{-3s})^{-1} \\
p \cdot \mathcal{H} \text{ has order 2} & (2,3) & (\alpha\beta) & (1 - p^{-s})^{-1}(1 - p^{-2s})^{-1}
\end{array}
\]

14. DEDEKIND’S CALCULATIONS

In Section 6 Dedekind introduces “Dirichlet’s ideal function \( J \)”, which today is called Dedekind’s zeta function \( \zeta_K(s) \).

Let \( F(p) \) denote the product of the contributions of the prime ideals above \( p \) to the Euler product; then \( \zeta_K(s) = \prod_p F(p) \), and by the decomposition law, the factors \( F(p) \) are determined as follows. Setting

\[
P_n = \left(1 - \frac{1}{p^{ns}}\right)^{-1}
\]

we have

\[
F(p) = \begin{cases} 
P_1 & \text{if } p \mid k; \\
\frac{P_1}{p^2} & \text{if } p = 3, \ 3 \nmid k; \\
P_1P_2 & \text{if } p \mid D, \ p \equiv 2 \mod 3; \\
\frac{P_1}{p} & \text{if } p \mid D, p \equiv 1 \mod 3, (m/p)_3 = 1; \\
P_1 & \text{if } p \mid D, p \equiv 1 \mod 3, (m/p)_3 \neq 1.
\end{cases}
\]

In the first four cases, \( F(p) \) contains the factor \( P_1 \); in the last case it follows from the identity

\[
1 - x^3 = (1 - x)(1 + x + x^2) = (1 - x)(1 - px)(1 - p^2x),
\]

where \( \rho = \frac{1 + \sqrt{-3}}{2} \) is a primitive cube root of unity, that \( P_3 \) can be written as the product of \( P_1 \) and the factor

\[
1 + \frac{1}{p} + \frac{1}{p^2} = 1 - \frac{1}{p} \frac{1}{1 - \frac{p}{p}}.
\]

Since \( \prod_p P_1 = \zeta(s) \) is the Riemann zeta function, this implies that \( \zeta_K(s) = \zeta(s) \cdot F(s) \) for a certain function \( F \) whose Euler factors follow from the above considerations.

In order to understand the Euler factorization of the function \( F(s) \), Dedekind considers the quadratic number field \( \mathbb{Q}(\sqrt{-3}) \). The occurrence of this field is easy to explain: if \( K/\mathbb{Q} \) is an arbitrary extension, then its normal closure must contain \( \sqrt{\text{disc } K} \). In the case of pure cubic number fields, \( D = \text{disc } k = -3k^2 \) shows that the normal closure of \( K \) is \( \mathbb{Q}(\sqrt{-3}, \sqrt{m}) \).

Dedekind defines a character \( \psi \) in the ring \( \mathbb{Z}[\rho] \) by giving its values on prime numbers \( \pi \). For such a prime \( \pi \), let \( \chi(\lambda) = [\frac{\lambda}{\pi}] \) denote the cubic residue symbol in \( \mathbb{Z}[\rho] \).

\[
\psi(\pi) = \begin{cases} 
0 & \text{if } \pi \mid p \text{ and } p \mid k; \\
1 & \text{if } \pi = 1 - p \text{ and } 3 \nmid k; \\
\chi(ab^2) & \text{otherwise}.
\end{cases}
\]
Now it is easily verified that in all cases we have
\[
F(p) = \frac{1}{1 - \frac{1}{p^2}} \cdot \prod \frac{1}{1 - \frac{\psi(\pi)}{N(\pi)^s}},
\]
where the product is over all primes \(\pi | p\) (up to units). In particular,
\[
\zeta K(s) = \zeta(s) \cdot \prod \frac{1}{1 - \frac{\psi(\pi)}{N(\pi)^s}},
\]
where the product is over all nonassociated prime elements \(\pi\) in \(\mathbb{Z}[\rho]\). The second product \(H\) may be transformed into a series using the geometric series, which gives
\[
H = \sum \frac{\psi(\omega)}{N(\omega)^s}.
\]
Since each nonzero element has exactly 6 associates, all of which have the same norm, this can be written in the form
\[
6H = \sum \frac{\psi(\mu)}{N(\mu)^s},
\]
where \(\mu\) runs over all integers of \(\mathbb{Z}[\rho]\) coprime to \(k\).

Next Dedekind recalls the cubic reciprocity law first proved by Jacobi and Eisenstein and uses it to prove that the character \(\chi(\mu)\) only depends on the residue class of \(\mu \mod k\), and that if \(\mu\) is coprime to \(k\) and congruent to a rational number modulo \(\mathbb{Q}(\sqrt[3]{\alpha})/\mathbb{Q}(\rho)\), this computation would have been superfluous.

Now consider the sum \(\sum \psi(\mu)N(\mu)^{-s}\) over all coprime integers \(\mu\). The character \(\psi\) is constant on residue classes modulo \(k\), hence we can write the sum as \(\sum \psi(\nu) \sum N(\lambda)^{-s}\), where \(\nu\) runs through a coprime system of residue classes modulo \(k\) and \(\lambda\) over all elements with \(\lambda \equiv \nu \mod k\).

Since \(\psi(\nu) = \psi(r\nu)\) for all integers \(r\) coprime to \(\nu\), we now collect residue classes modulo \(k\) that only differ by an integral factor into a single set, that is, we let \(\lambda\) run through all elements \(\lambda = r\nu + k\alpha\), where \(r\) is an integer coprime to \(k\) and \(\alpha\) runs through \(\mathcal{O}_k\), and \(\nu\) over a system of representatives of the coprime residue classes modulo \(k\), where two classes are identified if they differ by an integral factor coprime to \(k\).

If we drop the condition that \(r\) be coprime to \(k\), we get sums containing more terms. It turns out, however, that these additional terms cancel each other, and therefore
\[
\sum \psi(\nu) \sum N(\lambda)^{-s} = \sum \psi(\nu) \sum N(\lambda')^{-s},
\]
where \(\lambda'\) runs through all elements of \(k_{\nu} = \nu\mathbb{Z} + k\mathcal{O}\). This set \(k_{\nu}\) is a \(\mathbb{Z}\)-module of rank 2 in \(\mathbb{Z}[\rho]\), and these modules form a group with respect to the multiplication \(k_{\nu}k_{\nu'} = k_{\nu\nu'}\). It is known that such modules correspond to binary quadratic forms with discriminant \(-3k^2\), and that the multiplication of modules corresponds to composition of forms. It turns out that the modules \(k_\nu, k_{\nu\nu}\) and \(k_{\nu\nu'}\) are all equivalent and correspond to the same form class, so instead of \(6H = \sum \psi(\nu)S(k_{\nu})\), where \(S(k_{\nu})\) is the sum over all elements in \(k_{\nu}\), we can write \(2H = \sum \psi(\nu)S(k_{\nu})\), where the summation is only over modules \(k_\nu\) that are not equivalent and where
\[
S(k_{\nu}) = \sum \frac{1}{Q_\nu(x, y)^s} = \zeta(s, Q_\nu)
is the Epstein zeta function.

Since the norms \( N\lambda \) for elements \( \lambda \in k_\nu \) correspond to elements represented by the associated form, we finally find

\[
2H = \sum \psi(\nu)\zeta(s, Q_\nu),
\]

where \( Q_\nu \) is a form corresponding to \( k_\nu \). Now

\[
2H = \sum \zeta(s, Q_\nu) + \rho\zeta(s, Q_\mu) + \rho^2\zeta(s, Q_\lambda),
\]

where \( \psi(\nu) = 1, \psi(\mu) = \rho \) and \( \psi(\lambda) = \rho^2 \). Since \( \zeta(s, Q_\mu) = \zeta(s, Q_\lambda) \) and \( \rho + \rho^2 = -1 \), this means that

\[
2H = \sum \zeta(s, Q_\nu) - \sum \zeta(s, Q_\mu).
\]

Thus we have written \( 2H \) as a \( \mathbb{Z} \)-linear combination of Epstein zeta functions.

In the special case \( d = -3 \cdot 6^2 \) this relation becomes

\[
(13) \quad \frac{\zeta_K(s)}{\zeta(s)} = L(s, \psi) = \frac{1}{2} \sum' \frac{1}{(x^2 + 27y^2)^s} - \frac{1}{2} \sum' \frac{1}{(4x^2 + 2xy + 7y^2)^s},
\]

where \( \sum' \) indicates that the summation is over all pairs of integers \((x, y) \neq (0, 0)\).

Note that along the way we have proved Euler’s conjecture: the primes represented by \( x^2 + 27y^2 \) are those satisfying \( \chi(\pi) = 1 \), where \( \pi = \pi_3 \) in \( \mathbb{Z}[\rho] \), and coincide with those for which \( \psi(p) = 1 \).

Euler’s conjecture may also be read off (13). In fact, if we write the right hand side of (13) as \( \sum a(n)n^{-s} \), then \( a(p) = 4 \) if \( p \equiv 1 \) mod 3 is represented by \( x^2 + 27y^2 \) (observe that there are four representations \((\pm x, \pm y)\)), and \( a(p) = -2 \) otherwise (since here only \((x, y)\) and \((-x, -y)\) are counted). The product of the Euler factors of the primes above \( p \) on the left hand side, on the other hand, are given by

\[
F_p(s) = \begin{cases} 
(1 + p^{-s} + \ldots)^2 = 1 + 2p^{-s} + \ldots & \text{if } \left(\frac{3}{p}\right) = 1, \\
\frac{1}{1 + p^{-s} + p^{-2s}} = (1 + \rho p^{-s} + \ldots)(1 + \rho^2 p^{-s} + \ldots) = 1 - p^{-s} + \ldots & \text{if } \left(\frac{3}{p}\right) \neq 1.
\end{cases}
\]

15. The Proof

As before, \( K = \mathbb{Q}(\sqrt[3]{m}) \) denotes a pure cubic field with discriminant \( \Delta = -3k^2 \) and fundamental unit \( \varepsilon > 1 \).

In [25, p. 280], Shanks wrote that in his article [7],

\[
\text{Dedekind gives a leisurely, careful and detailed account of the Dedekind functions } \zeta_K(s) \text{ for pure cubic fields.}
\]

16. Dedekind’s class number formula

Define Dedekind’s eta function by

\[
\eta(z) = e^{\frac{\pi iz}{12}} \prod_{n=1}^{\infty} (1 - e^{2\pi izn}),
\]

as well as the function

\[
H(z) = \eta(z)\eta(-z)\sqrt{i(z - \bar{z})},
\]

where \( \bar{z} \) denotes the complex conjugate of \( z \), and where we assume that \( z \) lies in the upper half plane.

CUBIC RESIDUACIY AND QUADRATIC FORMS 41
Dedekind zeta function  \( \zeta_K(s) \)

\[ \frac{\zeta_K(s)}{\zeta(s)} \xrightarrow{s \to 1} h \cdot \frac{2\pi \log \varepsilon}{k \sqrt{3}} \]

\[ L(s, \psi) \]


\[ L(s, \chi) \]

Epstein zeta functions  \( \sum c_j \zeta(s, Q_j) \)

\[ \text{Kronecker limit} \]

\[ 2\pi k \sqrt{3} \cdot \log \prod H(\omega_1) \prod H(\omega_0) \]

Figure 7. Dedekind’s Class number formula for pure cubic number fields

\[ \varepsilon^h = \prod \frac{H(\omega_1)}{H(\omega_0)} \]

Now fix the pure cubic field \( K = \mathbb{Q}(\sqrt[3]{ab^2}) \) with discriminant \( \Delta = -3k^2 \) and consider all triples \( A, B, C \) of integers with

\[ AC = k, \quad 1 \leq B < A, \quad \gcd(A, B^2 + BC + C^2) = 1. \]

To each such triple we associate the binary quadratic form

\[ Q(x, y) = N(Ax + (B + C \rho)y). \]

A little calculation shows that

\[ Q(x, y) = (A^2, A(2B - C), B^2 - BC + C^2) \]

is a quadratic form with discriminant \( \Delta = -3A^2C^2 = -3k^2 \). For each such form we call \( \omega = \frac{B + C \rho}{A} \) the root of \( Q \).

Now let \( p > 3 \) be a prime represented by \( Q \). Dedekind has shown that \( (k/p)_3 \) has the same value for all primes \( p \) represented by the form \( Q \). Let \( \omega_N \) run through the roots of the forms that represent primes \( p \) with \( (k/p)_3 \neq 1 \), and \( \omega_R \) through those with \( (k/p)_3 = 1 \). Then Dedekind’s main result on the class numbers of pure cubic fields may be stated as follows:

**Theorem 16.1.** Let \( K = \mathbb{Q}(\sqrt{m}) \) be a pure cubic number field, and let \( \varepsilon > 1 \) denote its fundamental unit. Then the class number \( h = h_K \) is determined by

\[ \varepsilon^{6h} = \prod \frac{H(\omega_N)}{H(\omega_R)}. \]

This result was used by Harvey Cohn [4] in the late 1950s for computing class numbers of pure cubic number fields. In [5], he used this expression for proving that the class number \( h \) of pure cubic fields with discriminant \( D \) is asymptotically bounded by \( h = O(|d|^{1/2} \log \log |D|) \).

17. The Class-Number-1 Problem

As a testimony to the depth of Dedekind’s approach let me finally sketch the connection with Heegner’s solution of Gauß’s class-number-1 problem, which is taken from [22]. Assume that \( k = \mathbb{Q}(\sqrt{d}) \) with \( d \leq -11 \) is a complex quadratic number field with class number 1.
Since the minimal integral non-square norm in $k$ is $\frac{1+11}{4} = 3$, the prime ideal 2 must be inert, which implies $d \equiv 5 \mod 8$.

Then the number of forms with discriminant $4d$ is given by

$$h(4d) = \frac{\Phi(4)}{2\varphi(4)} = \frac{12}{4} = 3.$$ 

Let $K$ be the associated ring class field and $\mathcal{K}$ its real cubic subfield, and let $\varepsilon$ denote the fundamental unit of $K$. As in Dedekind’s case there is a class number formula of the type

$$\varepsilon^h = \prod H(\omega_1) \prod H(\omega_2).$$

The expression on the right hand side may be written as $\frac{1}{2} f(\sqrt{d})^3$; here $f$ is Schlöfli’s modular function defined by $f(\tau) = e^{-\pi i/24} \eta(\frac{\tau}{1+2})/\eta(\tau)$, where $\eta$ is Dedekind’s $\eta$ function.

Weber conjectured that $K = \mathbb{Q}(f(\sqrt{d})^3)$, and Heegner’s proof was not accepted at first because it was believed that his proof was based on this conjecture in an essential way. Weber knew that $K = \mathbb{Q}(f(\sqrt{d})^2)$, and this implies that we actually have $K = \mathbb{Q}(f(\sqrt{d}))$.

In fact it can be shown that $f(\sqrt{d})$ is an element of $K$ with norm 2.

Using Weber’s function

$$\gamma_2(\tau) = \sqrt[j]{f(\tau)} = \frac{f(\tau)^{24} - 2^4}{f(\tau)^8}$$

this leads the observation that $g = -\gamma_2(-\frac{3+\sqrt{d}}{2})$ is a natural number, and that the polynomial

$$X^{24} - 9X^{16} - 2^8 \in \mathbb{Z}[X]$$

splits into four irreducible factors of degrees 12, 6, 3 and 3. The conditions on the coefficients of these factors leads quickly to the solvability of the diophantine equation

$$y^2 = 2x(x^3 - 1)$$

in integers. The five integral solutions then give rise to the five complex quadratic number fields $\mathbb{Q}(\sqrt{d})$ with $d \leq -11$ and class number 1.

**References**

[8] L. Euler, Tractatus de numerorum doctrina capita sedecim quae supersunt, Comment. Arithm. 2 (1849), 503–575; E792, Opera Omnia V, 182–283; sh. S.

MÖRKKEWEG 1, 73489 JAGSTZELL, GERMANY
E-mail address: hb3@ix.urz.uni-heidelberg.de