Advanced Studies in Pure Mathematics 30, 2001
Class Field Theory – Its Centenary and Prospect
pp. 415–417

Class Numbers of Imaginary Quadratic Fields

Winfried Kohnen

§1. Introduction

Starting with Gauss, class numbers of quadratic fields always have been very interesting and quite mysterious objects. Here we would like to survey some more recent results concerning indivisibility of class numbers of imaginary quadratic fields by prime numbers. For more details we refer the reader to [1].

In the following, we denote by $D < 0$ the discriminant of an imaginary quadratic field. We let $h(D)$ be the class number, i.e. the order of the class group $CL(D)$ of $\mathbf{Q}(\sqrt{D})$.

We want to study the question "how often" $h(D)$ is not divisible by a given prime number l.

§2. Classical results

Theorem (Gauss). *Let t be the number of different prime divisors of D. Then $h(D)$ is odd if and only if $t = 1$.*

In fact, by genus theory one has $CL(D)/CL(D)^2 \cong (\mathbf{Z}/2\mathbf{Z})^{t-1}$. Now use the structure theorem for finite abelian groups.

Theorem (Hartung, 1974). *Let l be an odd prime. Then there exist infinitely many $D < 0$ such that $h(D) \not\equiv 0 \pmod{l}$.*

Let us sketch the *proof.* For a natural number N with $N \equiv 0, 3 \pmod 4$ let $H(N)$ be the Hurwitz-Kronecker class number, i. e. the class number of positive definite binary quadratic forms of discriminant $-N$ where each class C is counted with multiplicity $\frac{1}{\sharp Aut(C)}$. If $-N = Df^2$ with $f \in \mathbf{N}$ and D a fundamental discriminant, then

$$H(N) = \frac{h(D)}{w(D)} \sum_{d|f} \mu(d)(\frac{D}{d})\sigma_1(\frac{f}{d}),$$

Received September 21, 1998.

where $w(D)$ is half the number of units of $\mathbf{Q}(\sqrt{D})$ and $\sigma_1(n) = \sum_{d|n} d$.

By the Hurwitz-Kronecker class number relation one has

$$\sum_{|x|<2\sqrt{n}} H(4n - x^2) = \sum_{d|f} \max\{d, \frac{n}{d}\} \qquad (n \text{ not a perfect square}).$$

Now choose n to be a prime different from l such that $n \equiv 7 \pmod 8$ and n is not congruent to a perfect square modulo q for all odd primes $q < P$, where P is an arbitrary large number. We then conclude that there is x with $x^2 < 4n$ and $H(4n - x^2) \not\equiv 0 \pmod l$. Writing $4n - x^2 = -Df^2$ we see that also $h(D)$ is not divisible by l, and from the conditions posed on n one must have $|D| > P$. This concludes the proof.

§3. More recent results

Theorem (Horie, 1990). *Let $\epsilon_1, \cdots, \epsilon_n \in \{\pm 1, 0\}$ and $l_1, \cdots, l_n$ be different odd primes. Then for all primes l large enough there exist infinitely many $D < 0$ such that*

$$h(D) \not\equiv 0 \pmod l, \quad (\frac{D}{l_\nu}) = \epsilon_\nu (\nu = 1, \cdots, n).$$

The *proof* uses the theory of modular forms and the trace formula for Hecke operators.

Horie's theorem in general is not effective, and various refinements concerning effectiveness using the theory of modular forms of half-integral weight modulo l have recently been given, including works by Jochnowitz (1997) and most recently Bruinier (1997/98). Bruinier's results assert that the statement in Horie's theorem is true whenever l does not divide $\Pi_{\nu=1}^n l_\nu (l_\nu + 1)(l_\nu - 1)$.

However, these methods do not seem to give any reasonable lower bound for the number of D with $-x < D < 0$ and $h(D) \not\equiv 0 \pmod l$ for large x. On the other hand, there is the following

Conjecture (Cohen-Lenstra, 1983). *Let l be an odd prime. Then the probability that l does not divide $h(D)$ is $\Pi_{\nu=1}^n (1 - l^{-\nu})$.*

One knows that $\{D < 0 \mid h(D) \not\equiv 0 \pmod 3\}$ has a positive probability (Davenport-Heilbronn, 1971 and Nakagawa-Horie, 1988). For primes $l > 3$, however, nothing is known.

Theorem (Kohnen-K. Ono, 1997). *Let $l > 3$ be a prime. Then the following assertions hold.*

i) *Let p be any prime with $p \not\equiv (\frac{-4}{p}) \pmod{l}$. Then there exists $d_p \in \mathbf{N}$ with $d_p < \frac{3}{4}(p+1)$ such that $D := -pd_p$ or $D := -4pd_p$ is a fundamental discriminant and l does not divide $h(D)$.*

ii) *Let $\epsilon > 0$. Then*

$$\sharp\{-x < D < 0 \mid h(D) \not\equiv 0 \pmod{l}\} \geq (\frac{2(l-2)}{\sqrt{3}(l-1)} - \epsilon)\frac{\sqrt{x}}{\log x}(x >>_\epsilon 0).$$

The *proof* of i) uses properties of certain Hecke operators on spaces of modular forms of half-integral weight modulo l together with a theorem of Sturm which gives a bound on the dimension of spaces of modular forms reduced modulo l. The assertion of ii) follows from i) by using the prime number theorem. For details we refer to [1].

References

[1] Kohnen, W. and Ono, K., *Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication*, Invent. Math., **135** (1999), 387–398.

Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 288
69120 Heidelberg
Germany
E-mail address: winfried@mathi.uni-heidelberg.de