A Note on the Class Number of Imaginary Quadratic Fields*

By Raymond G. Ayoub†

1. Introduction. The object of this note is to make some observations on imaginary quadratic fields with a given class number. We give a different proof of a modified form of the theorem of Heilbronn and Linfoot [1] to the effect that there are at most 10 imaginary quadratic fields with class number 1. The nine known fields have discriminants -3, -4, -7, -8, -11, -19, -43, -67, -163. The existence or nonexistence of a 10th field remains an unsolved problem. We hasten to add that the arguments given below shed no new light on this famous problem.

Let $h(d)$ be the class number of the imaginary quadratic field $Q(\sqrt{-D})$ with $D > 0$ and square free and with discriminant $-d = -D$ or $-4D$.

Heilbronn [2] proved the famous conjecture of Gauss that $h(d) \to \infty$ as $d \to \infty$, and C. L. Siegel [3] proved the stronger result that for every $\epsilon > 0$, there exists a constant $d(\epsilon)$ such that for $d > d(\epsilon)$,

$$h(d) > d^{1/2-\epsilon}.$$

Both these results imply of course that the number of fields with a given class number must be finite; in particular there exists d_0 such that for $d > d_0$, $h(d) > 1$. Unfortunately, the constant d_0 cannot be effectively determined from either proof.

The proof of the theorem of Heilbronn and Linfoot was effected by modifying Heilbronn's proof of Gauss's conjecture, keeping control of the error, and it might be expected that Siegel's proof can be similarly modified, as indeed it can. We therefore prove the following:

Theorem A. *There exists an effectively calculable constant p_0 such that if $p_1 \geqq p_2 \geqq p_0$ and*

$$h(p_1) = h(p_2) = 1,$$

then $p_1 = p_2$.

It should perhaps be noted that if $h(d) = 1$, then d is a prime.

We shall defer for the time being an explicit evaluation of p_0. As we shall see in the course of the proof, we have a parameter at our disposal which may be expected to aid in determining the most economical value of p_0.

By modifying our proof somewhat, we can prove the slightly more general

Theorem B. *For any integer $h_0 \geqq 1$, there exists an effectively calculable constant $p_0(h_0)$ such that if*

$$d_1 \geqq d_2 \geqq p_0(h_0)$$

and

Received July 11, 1966. Revised November 21, 1966.

* This research was supported by the National Science Foundation under grant #GP-5593.

† The author is grateful to the referee for his helpful suggestions and for pointing out several errors in the original manuscript.

$$h(d_1) = h(d_2) = h_0\,,$$

then

$$d_1 = d_2\,.$$

We restrict our attention to a proof of Theorem A.

2. Proof of Theorem A. The proof is as noted above an adaptation of Siegel's argument. We shall state the results needed.

Let K be an algebraic extension of the rationals of degree n with γ_1 real and $2\gamma_2$ complex conjugates where $\gamma_1 + 2\gamma_2 = n$. Put $q = \gamma_1 + \gamma_2$, and let $x_1, x_2, \cdots, x_n$ be n positive real variables subject to the restriction that $x_{\gamma_2+l} = x_l$ ($l = \gamma_1 + 1, \cdots, \gamma_1 + \gamma_2$).

Let

$$N(x) = \prod_{i=1}^{n} x_i \quad \text{and} \quad S(x) = \sum_{i=1}^{n} x_i$$

and let

$$\zeta_K(s) = \sum_{\mathfrak{A}} \frac{1}{N(\mathfrak{A})^s}$$

be the Dedekind zeta function for the field K, where $\mathfrak{A}$ runs over the ideals of K and $N(\mathfrak{A})$ denotes the norm of the ideal $\mathfrak{A}$. Hecke (see e.g. Landau [4]) derived the functional equation for $\zeta_K(s)$ via the formula

$$\begin{aligned} \phi(s) &= \pi^{-ns/2} 2^{-\gamma_2 s} |d|^{s/2} \Gamma^{\gamma_1}\left(\frac{s}{2}\right) \Gamma^{\gamma_2}(s) \zeta_K(s) \\ &= \frac{\lambda_K}{s(s-1)} + \sum_{\mathfrak{A}} \int \cdots \int (N(x)^{s/2} + N(x)^{(1-s)/2}) \\ &\quad \times \exp\,[-\pi N(\mathfrak{A})^{2/n} |d|^{-1/n} S(x)]\, \frac{dx_1 \cdots dx_q}{x_1 \cdots x_q} \end{aligned} \tag{1}$$

where

$$\lambda_K = (2\pi)^{-\gamma_2} |d|^{1/2} \alpha\,, \tag{2}$$

d is the discriminant of K and α is the residue of $\zeta_K(s)$ at its simple pole at $s = 1$. The integration is over the domain $N(x) \geqq 1$.

The first inference to be drawn from (1) is that for $0 < s < 1$,

$$\phi_K(s) > \frac{\lambda_K}{s(s-1)} + |d|^{s/2} \exp\,[-2\pi n] 2^{-n}\,. \tag{3}$$

The proof is straightforward; the integrand being positive, we neglect all but the term $\mathfrak{A} = (1)$ in the sum and integrate only over $|d|^{1/n} \leqq x_i \leqq 2|d|^{1/n}$ ($i = 1, 2, \cdots, q$). Though the constant $\exp\,[-2\pi n]2^{-n}$ may be improved considerably, the order of magnitude as a function of $|d|$ may not. It should perhaps be remarked that it would be interesting to find a proof of (3) which does not use (1).

Now let d be the discriminant of a quadratic field and let

$$\chi_d(n) = (d/n)$$

be the Kronecker symbol; let

$$L(s, \chi_d) = \sum_{n=1}^{\infty} \frac{\chi_d(n)}{n^s} \tag{4}$$

be the L-function belonging to the primitive character χ_d.

If K is a quadratic field with discriminant $-d$ $(d > 0)$ with class number $h(d)$, then

$$\zeta_K(s) = \zeta(s) L(s, \chi_d) \tag{5}$$

and moreover in this case

$$L(1, \chi_d) = (\pi/\sqrt{d})\, h(d)\,. \tag{6}$$

These are well-known results (see e.g. Ayoub [6, Chapter V]). Assume now that K_1 and K_2 are imaginary quadratic fields with class number 1 and suppose that their discriminants are $-p_1$ and $-p_2$, where, as remarked above, p_1 and p_2 are primes. Suppose that K_3 is the quadratic field generated by $(p_1p_2)^{1/2}$ and suppose also that K is the biquadratic field generated by $(-p_1)^{1/2}$ and $(-p_2)^{1/2}$, that is by K_1 and K_2. Then since $p_i \equiv 3 \pmod 4$ for $p_i > 8$, it is a simple calculation to show that the discriminant of K_3 is p_1p_2, the discriminant of K is $(p_1p_2)^2$ and moreover for K we have $\gamma_2 = 2$ and of course $\gamma_1 = 0$. An examination of the decomposition of rational primes p in the field K yields the result (see Siegel [3])

$$\zeta_K(s) = \zeta(s) L(s, \chi_{-p_1}) L(s, \chi_{-p_2}) L(s, \chi_{p_1p_2})\,. \tag{7}$$

Since K_1 is assumed to have class number 1, it follows from (2), (5) and (6) that $\lambda_{K_1} = \frac{1}{2}$. If then $\varphi_{K_1}(s) \leqq 0$, then from (3) we should get

$$1 > s(1-s) p_1^{s/2} \exp[-4\pi] 2^{-1}\,. \tag{8}$$

Consequently if $s_0 \in (3/4, 1)$, we can find $p_0'(s_0)$ for which (8) is false. Therefore, for $p_1 \geqq p_0'(s_0)$ we have $\varphi_{K_1}(s_0) > 0$. In other words,

$$L(s_0, \chi_{-p_1}) \zeta(s_0) > 0\,.$$

But since $\zeta(s) < 0$ for $0 < s < 1$, it follows that

$$L(s_0, \chi_{-p_1}) < 0\,.$$

Since $L(1, \chi_{-p_1}) > 0$ from (5), (and $L(s, \chi)$ is continuous) we infer that there exists s_1, with $s_0 < s_1 < 1$, such that

$$L(s_1, \chi_{-p_1}) = 0\,. \tag{9}$$

We now apply (3) together with (7), using (9), to get

$$0 > \frac{\lambda_K}{s_1(s_1 - 1)} + c_1 (p_1p_2)^{s_1}\,, \tag{10}$$

where by (7), we have

$$\lambda_K = (2\pi)^{-2} 2 p_1 p_2 L(1, \chi_{-p_1}) L(1, \chi_{-p_2}) L(1, \chi_{p_1p_2})\,. \tag{11}$$

On the other hand, if χ is a real character mod k, then we have the inequality

$$L(1, \chi) < 3 \log k = c_2 \log k \tag{12}$$

which is readily derived by partial summation.

We use (6) for $L(1, \chi_{-p_1})$ and $L(1, \chi_{-p_2})$ and (12) for $L(1, \chi_{p_1 p_2})$ in (10) and (11) and infer that

$$0 > \frac{c_3 (p_1 p_2)^{1/2} \log p_1 p_2}{s_1(s_1 - 1)} + c_4 (p_1 p_2)^{s_1}$$

or

$$\log p_1 p_2 > c_5 s_1 (1 - s_1)(p_1 p_2)^{s_1 - 1/2} . \tag{13}$$

It is elementary to show that there exists a constant c_6 such that

$$1 - s_1 > c_6 / (p_1)^{1/2} \log p_1 \tag{14}$$

but we shall use the much deeper result of Rosser [5], viz.

$$1 - s_1 > \pi/6 \; (p_1)^{1/2} \tag{15}$$

even though (14) could be used for numerical purposes. Putting (15) in (13), we get for $p_1 > p_0'(s_0)$

$$\log p_1 p_2 > c_7 (p_1 p_2)^{s_0 - 1/2} p_1^{-1/2} . \tag{16}$$

The entire argument, however, is symmetric in p_1 and p_2, and we therefore infer that for $p_2 > p_0''(s_0)$

$$\log p_1 p_2 > c_8 (p_1 p_2)^{s_0 - 1/2} p_2^{-1/2} . \tag{17}$$

From (16) and (17) it now follows that if $p_1, p_2 > p_0'''(s_0) = \max (p_0', p_0'')$, then

$$\log^2 p_1 p_2 > c_9 (p_1 p_2)^{2 s_0 - 3/2} . \tag{18}$$

Since we assumed that $s_0 > 3/4$, (18) leads to a contradiction if $p_1, p_2 > p_0^{(\mathrm{iv})}(s_0)$. Thus, finally, if $p_0(s_0) = \max (p_0''', p_0^{(\mathrm{iv})})$, we get a contradiction—hence $p_1 = p_2$.

It should be noted finally that all of the constants $c_1, c_2, \cdots, c_9$ as well as the p_0's are effectively calculable.

Moreover it should be observed that in numerical calculations, we have in addition the parameter s_0 at our disposal.

Pennsylvania State University
University Park, Pennsylvania

1. H. Heilbronn & E. H. Linfoot, "On imaginary quadratic corpora of class number 1," *Quart. J. Math. Oxford.*, v. 5, 1934.

2. H. Heilbronn, "On the class number in imaginary quadratic fields," *Quart. J. Math. Oxford*, v. 5, 1934.

3. C. L. Siegel, "Über die Klassenzahl imaginärquadratische Zahlkörper," *Acta Arith.*, v. 1, 1936.

4. E. Landau, *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*, reprint of 2nd ed., Chelsea, New York, 1949. MR 11, 85.

5. B. Rosser, *Real Roots of Real Dirichlet L-Series*. II, United States Air Force Office of Scientific Research, Report #72, 1957.

6. R. Ayoub, *An Introduction to the Analytic Theory of Numbers*, Math. Surveys, No. 10, Amer. Math. Soc., Providence, R. I., 1963.