ON THE CLASS NUMBER OF CERTAIN IMAGINARY QUADRATIC FIELDS

J. H. E. COHN

(Communicated by David E. Rohrlich)

Abstract. Theorem. Let \( n > 2 \) denote an integer, \( D \) the square-free part of \( 2^n - 1 \) and \( h \) the class number of the field \( \mathbb{Q}[\sqrt{-D}] \). Then except for the case \( n = 6 \), \( n - 2 \) divides \( h \).

Theorem. Let \( n > 2 \) denote an integer, \( D \) the square-free part of \( 2^n - 1 \) and \( h \) the class number of the field \( \mathbb{Q}[\sqrt{-D}] \). Then except for the case \( n = 6 \), \( n - 2 \) divides \( h \).

This generalises Theorem 5.3 of \[2\], which derives the same conclusion under the restrictions that \( n - 2 \) be squarefree and coprime to 6, and provides a new proof of the result in \[1\] that for each \( g \) there are infinitely many imaginary quadratic fields whose class number is divisible by \( g \).

Proof. Here the Diophantine Equation \( 2^n - 1 = Da^2 \) has at least one solution, with \( a \) odd and \( D \equiv 7 \pmod{8} \); in particular \( D \geq 7 \) and so the only units in the field are \( \pm 1 \). Thus in the field we obtain \( \left(\frac{1}{2}(1 + a\sqrt{-D})\right)\left(\frac{1}{2}(1 - a\sqrt{-D})\right) = 2^{n-2} \) where the ideal \( \left[\frac{1}{2}(1 + a\sqrt{-D})\right] \) and its conjugate are coprime; thus \( \left(\frac{1}{2}(1 + a\sqrt{-D})\right) = \pi^{n-2} \) for an ideal \( \pi \) having norm 2. Let \( \lambda = (h, n-2) \) with \( h = \lambda \mu, n-2 = \lambda \nu \) and \( (\mu, \nu) = 1 \).

Since the ideal \( \pi^h \) is principal, it follows that \( \left(\frac{1}{2}(1 + a\sqrt{-D})\right)^{\mu} = \pi^{\lambda \nu} = (\pi^h)^{\nu} = [\delta]^\nu \) for some algebraic integer \( \delta \) in the field, and so \( \left(\frac{1}{2}(1 + a\sqrt{-D})\right)^{\mu} = \pm \delta^{\nu} \). In view of \( (\mu, \nu) = 1 \), it then follows that \( \frac{1}{2}(1 + a\sqrt{-D}) = \pm \gamma^{\nu} \) for some other algebraic integer in the field, \( \gamma \). It merely remains to show that \( \nu = 1 \), for then \( n - 2 = \lambda \mu = h \).

We show first that \( \nu \) has no odd prime factor \( p \), for otherwise we should find, absorbing the \( \pm \) sign into the right-hand side, that for some odd rational integers \( \alpha \) and \( \beta, \frac{1}{2}(1 + a\sqrt{-D}) = (\frac{1}{2}(\alpha + \beta\sqrt{-D}))^p \), and then equating real parts gives

\[
2^{p-1} = \alpha \sum_{r=0}^{\frac{p-1}{2}} \binom{p}{2r} \alpha^{p-2r-1}(-D\beta^2)^r.
\]

This would imply \( \alpha = \pm 1 \) and then \( \pm 2^{p-1} = \sum_{r=0}^{\frac{p-1}{2}} \binom{p}{2r}(-D\beta^2)^r \), with the lower sign rejected modulo \( p \). Thus \( 2^{p-1} = \frac{1}{2}((1 + \sqrt{-D})^p + (1 - \sqrt{-D})^p) = f_p(x) \),

Received by the editors October 31, 2000.
2000 Mathematics Subject Classification. Primary 11R29; Secondary 11D61, 11B37, 11B39.

\( \odot2001 \) American Mathematical Society

1275
say, where \( x = 1 + D\beta^2 \equiv 0 \pmod{8} \), and we show that this is impossible for any odd integer \( p \), by showing that for each odd \( k \geq 3 \)

\[
\left( 1 + \sqrt{1 - x} \right)^2 + \left( 1 - \sqrt{1 - x} \right)^2 = 4 - 2x \quad \text{and} \quad \left( 1 + \sqrt{1 - x} \right)^2 \left( 1 - \sqrt{1 - x} \right)^2 = x^2,
\]
we obtain the recurrence relation \( f_{k+4}(x) = (4 - 2x)f_{k+2}(x) - x^2 f_k(x) \) with the values \( f_3(x) = 4 - 3x \) and \( f_5(x) = 16 - 20x + 5x^2 \). Thus (1) holds for these values since \( 8 \mid x \), and we proceed to prove it by induction for larger \( k \). If it holds for odd values \( t \) and \( t + 2 \), then

\[
f_{t+4}(x) = (4 - 2x)f_{t+2}(x) - x^2 f_t(x)
= (4 - 2x)(2^{t+1} - (t + 2)x \cdot 2^{t-1} + Ax \cdot 2^{t-2})
= x^2(2^{t+1} - tx \cdot 2^{t-3} + Bx \cdot 2^{t-2})
= 2^{t+3} - (t + 4)x \cdot 2^{t+1} + Cx \cdot 2^{t-1},
\]
say, where \( C = A + \frac{3}{4}(t + 2) - \frac{4}{15}Ax - \frac{1}{7}x^2 + \frac{1}{12}tx^2 - \frac{1}{15}Bx^2 \) is an integer.

Thus \( \nu \) has no odd prime factor. Finally suppose that \( 2 \mid \nu \). Then we obtain that \( \pm 2(1 + a\sqrt{-D}) = (\alpha + \beta\sqrt{-D})^2 \), since now the unit \( \pm 1 \) can no longer be absorbed into the power. Then \( \pm 2 = \alpha^2 - D\beta^2, \pm \alpha = \alpha\beta \). But since \( D \equiv 7 \pmod{8} \) we must reject the lower sign in the former, and then find

\[
2^n = 1 + Da^2 = 1 + D\alpha^2 \beta^2 = \alpha^4 - 2\alpha^2 + 1 = (\alpha^2 - 1)^2
\]
and so \((\alpha + 1)(\alpha - 1) = 2^k \) whence for some integers \( i > j, \alpha + 1 = 2^i, \alpha - 1 = 2^j, 2 = 2^i - 2^j \), yielding only \( i = 2, j = 1, \alpha = 3 \), leading to \( n = 6 \) and \( D = 7 \) as required.

The author wishes to express his appreciation to the referee for providing the references, and for suggesting an improvement in the exposition.

A table showing the first few values of \( h/(n - 2) \) is given in Table 1.
REFERENCES


DEPARTMENT OF MATHEMATICS, ROYAL HOLLOWAY UNIVERSITY OF LONDON, EGHAM, SURREY TW20 0EX, UNITED KINGDOM

E-mail address: J.Cohn@rhul.ac.uk