PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 130, Number 5, Pages 1275–1277
S 0002-9939(01)06255-4
Article electronically published on October 5, 2001

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 $Q[\sqrt{-D}]$. 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 $Q[\sqrt{-D}]$. 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 ± 1. Thus in the field we obtain $(\frac{1}{2}(1 + a\sqrt{-D}))(\frac{1}{2}(1 - a\sqrt{-D})) = 2^{n-2}$ where the ideal $[\frac{1}{2}(1+a\sqrt{-D})]$ and its conjugate are coprime; thus $[\frac{1}{2}(1+a\sqrt{-D})] = \pi^{n-2}$ for an ideal π having norm 2. Let $\lambda = (h, n-2)$ with $h = \lambda\mu$, $n-2 = \lambda\nu$ and $(\mu, \nu) = 1$. Since the ideal π^h is principal, it follows that $[\frac{1}{2}(1+a\sqrt{-D})]^\mu = \pi^{\lambda\mu\nu} = (\pi^h)^\nu = [\delta]^\nu$ for some algebraic integer δ in the field, and so $(\frac{1}{2}(1+a\sqrt{-D}))^\mu = \pm\delta^\nu$. 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, γ. It merely remains to show that $\nu = 1$, for then $n-2 = \lambda|\lambda\mu = h$.

We show first that ν 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 α and β, $\frac{1}{2}(1 + a\sqrt{-D}) = (\frac{1}{2}(\alpha + \beta\sqrt{-D}))^p$, and then equating real parts gives

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

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

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

Table 1.

n	$h/(n-2)$	n	$h/(n-2)$	n	$h/(n-2)$
3	1	15	4	27	156
4	1	16	8	28	384
5	1	17	19	29	480
6	1/4	18	4	30	280
7	1	19	15	31	685
8	2	20	8	32	1408
9	2	21	6	33	1776
10	2	22	44	34	1982
11	2	23	74	35	1728
12	2	24	24	36	1792
13	5	25	164	37	6108
14	6	26	202		

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 $k \geq 3$

(1) $$f_k(x) \equiv 2^{k-1} - kx \cdot 2^{k-3} \pmod{x \cdot 2^{k-2}}.$$

Since $(1+\sqrt{1-x})^2+(1-\sqrt{1-x})^2 = 4-2x$ and $(1+\sqrt{1-x})^2(1-\sqrt{1-x})^2 = x^2$, 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 $8|x$, and we proceed to prove it by induction for larger k. If it holds for odd values t and $t+2$, then

$$\begin{aligned} f_{t+4}(x) &= (4-2x)f_{t+2}(x) - x^2 f_t(x) \\ &= (4-2x)(2^{t+1} - (t+2)x \cdot 2^{t-1} + Ax \cdot 2^t) \\ &\quad - x^2(2^{t-1} - tx \cdot 2^{t-3} + Bx \cdot 2^{t-2}) \\ &= 2^{t+3} - (t+4)x \cdot 2^{t+1} + Cx \cdot 2^{t+2}, \end{aligned}$$

say, where $C = A + \frac{x}{4}(t+2) - \frac{1}{2}Ax - \frac{1}{8}x + \frac{1}{32}tx^2 - \frac{1}{16}Bx^2$ is an integer.

Thus ν has no odd prime factor. Finally suppose that $2|\nu$. Then we obtain that $\pm 2(1 + a\sqrt{-D}) = (\alpha + \beta\sqrt{-D})^2$, since now the unit ± 1 can no longer be absorbed into the power. Then $\pm 2 = \alpha^2 - D\beta^2$, $\pm a = \alpha\beta$. 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 $(\alpha+1)(\alpha-1) = 2^{\frac{1}{2}n}$ 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

1. N. C. Ankeny and S. Chowla, *On the divisibility of the class numbers of quadratic fields*, Pacific J. Math. **5** (1955), 321–324. MR **19:**18f
2. B. H. Gross and D. E. Rohrlich, *Some results on the Mordell-Weil group of the Jacobian of the Fermat curve*, Inventiones Math. **44** (1978), 201–224. MR **58:**10911

Department of Mathematics, Royal Holloway University of London, Egham, Surrey TW20 0EX, United Kingdom

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