On the divisibility of the class number of imaginary quadratic fields

By Katsumasa Ishii

2-6-3-201 Miyasaka, Setagaya-ku, Tokyo 156-0051, Japan

(Communicated by Shigefumi Mori, M.J.A., Sept. 12, 2011)

Abstract: Let U be an integer with $U > 1$. If n is even with $n \geq 6$, then the class number of $\mathbf{Q}(\sqrt{1-4U^n})$ is divisible by n except $(U, n) = (13, 8)$.

Key words: Imaginary quadratic field; class number; divisibility.

Let U be an integer with $U > 1$. Gross and Rohrlich [2] proved that if n is odd with $n > 1$, then the class number of $\mathbf{Q}(\sqrt{1-4U^n})$ is divisible by n. Furthermore Louboutin [5] proved that if at least one of the prime divisors of an odd integer $U \geq 3$ is equal to 3 modulo 4, then the class number of $\mathbf{Q}(\sqrt{1-4U^n})$ is divisible by n. In this note we shall consider the same problem for the case where n is even with $n \geq 6$. We shall show the following

Theorem. *Let U be an integer with $U > 1$. If n is even with $n \geq 6$, then the class number of $\mathbf{Q}(\sqrt{1-4U^n})$ is divisible by n except $(U, n) =$ $(13, 8)$.*

In order to prove this, we need the following lemma.

Lemma 1. *Suppose that $k > 2$.*

1. *The Diophantine equation $x^2 - 2y^k = 1$ has no integer solutions other than $x = 1, y = 0$.*
2. *The only positive integer solutions of the Diophantine equation $x^2 - 2y^k = -1$ are $x = y = 1$ and $x = 239, y = 13, k = 4$.*

Proof. 2 is Lemma in [1]. Now we shall show 1. It suffices to show the case where $k = 4$ and k are odd primes. The case where $k = 4$ is in [6]. Suppose that k is an odd prime with $k > 3$. From $x^2 - 2y^k = 1$ we have $(x+1)(x-1) = 2y^k$. Since $(x+1, x-1) = 2$ (note that x is odd) and either $x+1$ or $x-1$ is not divisible by 4, we have $x \pm 1 = 2^{kt}u^k$ and $x \mp 1 = 2v^k$ for some t such that both u and v are odd with $(u, v) = 1$. Then we have $2^{kt}u^k - 2v^k = \pm 2$, that is, $2^{k-1}(2^{t-1}u)^k - v^k = \pm 1$. By Theorem 1 in [7], this equation has no integer solution for $k \geq 7$. For $k = 5$ this also has no integer solution by the fact that the non-trivial solution of $x^5 + 16y^5 = z^2$ is $(x, y, z) = (2, -1, 4)$ due to the arguement of Appendice in [4]. Finally consider the case where $k = 3$. From $x^2 - 2y^3 = 1$, we have $(2x)^2 - 4 = (2y)^3$. The only integer solution of the equation $x^2 - 4 = y^3$ is $x = 2, y = 0$ (for example, see [3]). □

Furthermore we shall use the following lemma from Louboutin [5]. As is usual, N and Tr denote the norm and the trace respectively.

Lemma 2 (Lemma 4 in [5]). *Let α be an integer in a quadratic field K. Then α is a square in K if and only if there exists a rational integer a such that $N(\alpha) = a^2$ and $Tr(\alpha) + 2a$ is a square.*

Proof of Theorem. First note that $\mathbf{Q}(\sqrt{1-4U^n}) \neq \mathbf{Q}(\sqrt{-1})$. In order to see that $\mathbf{Q}(\sqrt{1-4U^n}) \neq \mathbf{Q}(\sqrt{-3})$, consider the equation $1 - 4U^n = -3x^2$. We transform this to

$$\left(\frac{1+\sqrt{-3}x}{2}\right)\left(\frac{1-\sqrt{-3}x}{2}\right) = U^n.$$

Since n is even and the primitive cubic root of 1 is a square in $\mathbf{Q}(\sqrt{-3})$, $\pm(1+\sqrt{-3}x)/2$ is a square and hence $\pm 1 + 2U^{\frac{n}{2}} = a^2$ for some a by Lemma 2. Since $n \geq 6$, we have $a^2 - 2U^m = \pm 1$ with $m > 2$. This contradicts Lemma 1 since $U > 1$ and $U \neq 13$.

Now put $\alpha = (1 + \sqrt{1-4U^n})/2$. By the same argument in [5], it suffices to show that neither α nor $-\alpha$ are squares in $\mathbf{Q}(\sqrt{1-4U^n})$. If $\pm\alpha$ is a square, then $\pm 1 + 2U^{\frac{n}{2}} = a^2$ for some a by Lemma 2, a contradiction again. □

Remark. Note that the class number of $\mathbf{Q}(\sqrt{1-4\cdot 13^8}) = \mathbf{Q}(\sqrt{-6347})$ is 28.

2000 Mathematics Subject Classification. Primary 11R11.

doi: 10.3792/pjaa.87.142

References

[1] J. H. E. Cohn, Perfect Pell powers, Glasgow Math. J. **38** (1996), no. 1, 19–20.

[2] B. H. Gross and D. E. Rohrlich, Some results on the Mordell-Weil group of the Jacobian of the Fermat curve, Invent. Math. **44** (1978), no. 3, 201–224.

[3] O. Hemer, Notes on the Diophantine equation $y^2 - k = x^3$, Ark. Mat. **3** (1954), 67–77.

[4] W. Ivorra, Sur les équations $x^p + 2^\beta y^p = z^2$ et $x^p + 2^\beta y^p = 2z^2$, Acta Arith. **108** (2003), no. 4, 327–338.

[5] S. R. Louboutin, On the divisibility of the class number of imaginary quadratic number fields, Proc. Amer. Math. Soc. **137** (2009), no. 12, 4025–4028.

[6] L. J. Mordell, The Diophantine equation $y^2 = Dx^4 + 1$, J. London Math. Soc. **39** (1964), 161–164.

[7] S. Siksek, On the Diophantine equation $x^2 = y^p + 2^k z^p$, J. Théor. Nombres Bordeaux **15** (2003), no. 3, 839–846.