PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 12, December 2009, Pages 4025–4028
S 0002-9939(09)10021-7
Article electronically published on July 22, 2009

ON THE DIVISIBILITY OF THE CLASS NUMBER OF IMAGINARY QUADRATIC NUMBER FIELDS

STÉPHANE R. LOUBOUTIN

(Communicated by Ken Ono)

ABSTRACT. We prove that if at least one of the prime divisors of an odd integer $U \geq 3$ is equal to 3 mod 4, then the ideal class group of the imaginary quadratic field $\mathbf{Q}(\sqrt{1-4U^n})$ contains an element of order n.

1. INTRODUCTION

In 1953, N. C. Ankeny and S. Chowla proved in [AC] that for any given integer $n > 1$ there are infinitely many imaginary quadratic number fields of the form $\mathbf{Q}(\sqrt{x^2-3^n})$, with x^2-3^n square-free, whose class numbers are divisible by n. In 2008, Y. Kishi came back in [Ki] to this family and proved that in the case where $x = 4^k < 3^n$ is a power of 4, then n always divides the class number of $\mathbf{Q}(\sqrt{x^2-3^n})$. In 1978, B. H. Gross and D. E. Rohrlich delineated in [GR] a proof of the fact that for any given **odd** $n > 1$ there are infinitely many imaginary quadratic number fields whose class numbers are divisible by n, namely the imaginary quadratic fields $\mathbf{Q}(\sqrt{1-4U^n})$, $U > 1$. In 2002, J. H. E. Cohn came back in [Co] to this family and proved that $n \neq 4$, be it **odd or even**, always divides the class number of the imaginary quadratic fields $\mathbf{Q}(\sqrt{1-4\cdot 2^n})$. The aim of this note is (i) to expound Gross and Rohrlich's proof (the first point of Theorem 1) and (ii) to prove a result stronger than [GR, Theorem 5.3] (the second point of Theorem 1). However, we note that the family of imaginary quadratic number fields $\mathbf{Q}(\sqrt{1-4U^n})$ is much thinner than the families studied in [Mur] or [So]. Thus, our results, though pleasingly explicit, have no hope of approaching a proof of the Cohen-Lenstra heuristics, which state that the number $N_n(x)$ of imaginary quadratic fields $\mathbf{Q}(\sqrt{-d})$ with $0 < d < x$, d square-free, whose class groups contain elements of order n, is asymptotic to $C_n x$ as x tends to infinity, for some positive and explicit constant C_n.

Theorem 1. *Fix $n > 1$. Then:*

1. *If n is* **odd**, *then for any integer $U \geq 2$ the ideal class groups of the imaginary quadratic fields $\mathbf{Q}(\sqrt{1-4U^n})$ contain an element of order n.*
2. *If at least one of the prime divisors of an* **odd** *integer $U \geq 3$ is equal to 3 mod 4, then the ideal class group of the imaginary quadratic field $\mathbf{Q}(\sqrt{1-4U^n})$ contains an element of order n.*

Received by the editors March 20, 2009, and, in revised form, April 9, 2009.
2000 *Mathematics Subject Classification.* Primary 11R29; Secondary 11R11.
Key words and phrases. Class number, imaginary quadratic field, divisibility.

2. Being a pth power

Throughout this note, we let $\mathbf{k}$ be a quadratic number field. Let σ be its non-trivial $\mathbf{Q}$-automorphism. Let $\mathbf{A_k}$ be its ring of algebraic integers and let $d_\mathbf{k}$ be its discriminant. Let $Tr(\alpha) = \alpha + \sigma(\alpha) \in \mathbf{Z}$ and $N(\alpha) = \alpha\sigma(\alpha) \in \mathbf{Z}$ be the trace and norm of $\alpha \in \mathbf{A_k}$. Let $\mathbf{A_k}^*$ be the group of units of $\mathbf{A_k}$. We say that $\alpha \in \mathbf{A_k}$ is associated with $\beta \in \mathbf{A_k}$ if there exists $\eta \in \mathbf{A_k}^*$ such that $\beta = \eta\alpha$, i.e. if the principal ideal (β) of $\mathbf{A_k}$ is equal to (α).

Lemma 2. *Let $\alpha \in \mathbf{A_k}$. If $k \geq 1$ is odd, then $Tr(\alpha)$ divides $Tr(\alpha^k)$. If $p \geq 3$ is prime, then $Tr(\alpha^p) \equiv Tr(\alpha) \pmod p$. Hence, if $Tr(\alpha) = 1$ and if α is a pth power in $\mathbf{A_k}$, then α is a unit of $\mathbf{A_k}$.*

Proof. Since $\alpha^2 - Tr(\alpha)\alpha + N(\alpha) = 0$ with $Tr(\alpha) \in \mathbf{Z}$ and $N(\alpha) \in \mathbf{Z}$, we have $\alpha^{k+2} = Tr(\alpha)\alpha^{k+1} - N(\alpha)\alpha^k$ for $k \geq 0$, which, in taking the trace, yields the first result by induction on $k \geq 1$ odd. Since p divides the binomial coefficients $\binom{p}{l}$ for $1 \leq l \leq p-1$, we have $Tr(\alpha)^p - Tr(\alpha^p) = (\alpha + \sigma(\alpha))^p - \alpha^p - \sigma(\alpha)^p = \sum_{l=1}^{p-1} \binom{p}{l}\alpha^l\sigma(\alpha)^{p-l} \in p\mathbf{A_k} \cap \mathbf{Z} = p\mathbf{Z}$ and, using $Tr(\alpha)^p \equiv Tr(\alpha) \pmod p$, we obtain the second result. If $\alpha = (1 + y\sqrt{d_\mathbf{k}})/2 = \beta^p = ((u + v\sqrt{d_\mathbf{k}})/2)^p$ of trace equal to 1 is a pth power in $\mathbf{A_k}$, then $u = Tr(\beta)$ divides $1 = Tr(\alpha) = Tr(\beta^p)$ (the first point), hence $u = \pm 1$, and $u = Tr(\beta) \equiv Tr(\beta^p) = Tr(\alpha) = 1 \pmod p$ (the second point), hence $u = 1$. Then $\beta = (1 + v\sqrt{d_\mathbf{k}})/2 \in \mathbf{A_k}$ satisfies $\sigma(\beta) = 1 - \beta$; hence $\beta^p + (1-\beta)^p = Tr(\beta^p) = Tr(\alpha) = 1$ and

$$0 = (1-\beta)^p - 1 + \beta^p = \sum_{l=1}^{p-1} \binom{p}{l}(-\beta)^l = -p\beta\Big(1 - \beta\sum_{l=2}^{p-1} \frac{1}{p}\binom{p}{l}(-\beta)^{l-2}\Big).$$

Therefore, we have

$$\beta\sum_{l=2}^{p-1} \frac{1}{p}\binom{p}{l}(-\beta)^{l-2} = 1,$$

and β, hence α, is a unit of $\mathbf{A_k}$. □

Proposition 3. *Let $\mathbf{k}$ be an imaginary quadratic field. If $\alpha \in \mathbf{A_k}$ with $Tr(\alpha) = 1$ is associated with a pth power for some odd prime $p \geq 3$, then α is a unit of $\mathbf{A_k}$.*

Proof. If $\mathbf{k} \neq \mathbf{Q}(\sqrt{-3})$, or if $\mathbf{k} = \mathbf{Q}(\sqrt{-3})$ and $p > 3$, then any unit in $\mathbf{k}$ is a pth power, and the result follows from Lemma 2. Now assume that $\mathbf{k} = \mathbf{Q}(\sqrt{-3})$ and $p = 3$. Set $j = (-1 + \sqrt{-3})/2$. We have $\alpha = \beta^3$, $j\beta^3$ or $j^2\beta^3$ in $\mathbf{A_k}$, and $\alpha \neq \beta^3$, by Lemma 2. If $\beta = (u + v\sqrt{-3})/2$, with $u \equiv v \pmod 2$, then $1 = Tr(\alpha) = Tr(j\beta^3)$ yields $-8 = \Delta(u,v) = u(u^2 - 9v^2) + 9v(u^2 - v^2)$ and $1 = Tr(\alpha) = Tr(j^2\beta^3)$ yields $-8 = \Delta(u,-v)$. If $U = (u-3v)/2$ and $V = (u+3v)/2$, then $\beta = \big(U + V + \frac{V-U}{3}\sqrt{-3}\big)/2$, $\Delta(u,v) = -8(U^3 - 3UV^2 - V^3)/3$ and $\Delta(u,-v) = -8(V^3 - 3VU^2 - U^3)/3$. Hence, $U^3 - 3UV^2 - V^3 = 3$ or $V^3 - 3VU^2 - U^3 = 3$, which implies $(U,V) \in \{(-1,-1),(2,-1),(-1,2)\}$, $\beta = -1$, $-j$ or $-j^2$, $\beta^3 = -1$ and the desired result. Indeed, this is a Thue equation associated with the real cyclic cubic field $K = \mathbf{Q}(\alpha)$ of conductor 9, ring of algebraic integers $\mathbf{Z}[\alpha]$ and fundamental units $\eta_1 = \alpha$ and $\eta_2 = \alpha^2 - \alpha - 2$, where $\alpha^3 - 3\alpha - 1 = 0$ (we can also write this equation as $N(U - \alpha V) = 3$, i.e. $U - \alpha V$ must be associated with $-1 - \alpha$, of norm 3). Now, by using Bilu and Hanrot's method (see [BH]), such a Thue equation can easily be solved by program packages like Kash (see [DFKPRW, Section 7.3]). □

It remains to deal with the prime $p = 2$.

Lemma 4. *Let* $\mathbf{k}$ *be a quadratic number field. If* $\alpha \in \mathbf{A_k}$*, then* α *is a square in* $\mathbf{A_k}$ *if and only if there exists* $A \in \mathbf{Z}$ *such that* $N(\alpha) = A^2$ *and such that* $Tr(\alpha) + 2A$ *is a square in* $\mathbf{Z}$*. If* $\mathbf{k}$ *is imaginary, we may assume that* $A \geq 0$*.*

Proof. If $\alpha = \beta^2$, then $N(\alpha) = A^2$ with $A = N(\beta)$ (hence $A \geq 0$ if $\mathbf{k}$ is imaginary), and $Tr(\alpha) + 2A = Tr(\beta)^2 - 2N(\beta) + 2A = Tr(\beta)^2$ is a square. Conversely, if $N(\alpha) = A^2$ and $Tr(\alpha) + 2A = B^2$ are squares, then $\alpha^2 - Tr(\alpha)\alpha + N(\alpha) = 0$ yields $\alpha^2 - (B^2 - 2A)\alpha + A^2 = 0$, and $\alpha = ((B \pm \sqrt{B^2 - 4A})/2)^2$ is a square $\mathbf{A_k}$. □

3. Proof of Theorem 1

Set $\mathbf{k} = \mathbf{Q}(\sqrt{1 - 4U^n})$ and $\alpha = (1 + \sqrt{1 - 4U^n})/2 \in \mathbf{A_k}$. Then $Tr(\alpha) = 1$ and α is not a unit in $\mathbf{A_k}$ (for $N(\alpha) = U^n > 1$). Since $Tr(\alpha) = \alpha + \sigma(\alpha) = 1$, the principal ideals (α) and $(\sigma(\alpha))$ are relatively prime and their product $(U)^n$ is an nth power. Therefore, $(\alpha) = \mathbf{I}^n$ is the nth power of some ideal $\mathbf{I}$ of $\mathbf{A_k}$, and the ideal class of $\mathbf{I}$ is of order dividing n. Assume that it is not of order n. Then $\mathbf{I}^{n/p} = (\beta)$ is principal for some prime $p \geq 2$ dividing n. Hence $(\alpha) = (\beta^p)$ and α is associated with β^p, a pth power in $\mathbf{A_k}$. By Proposition 3, we have $p = 2$, which proves the first point of Theorem 1. Finally, assume that $U \geq 3$ is odd and that α is associated with a square. Since $\mathbf{k} \neq \mathbf{Q}(\sqrt{-1})$, α or $-\alpha$ is a square. Now, if α is a square, then we know by Lemma 4 that $1 + 2U^{n/2}$ is a square. But since U is odd, we know that $1 + 2U^{n/2} \equiv 3 \pmod 4$, so α cannot be a square. Thus, $-\alpha$ is a square, and we conclude that $-1 + 2U^{n/2}$ is a square by Lemma 4. It follows that for any prime $p \geq 3$ dividing U, $-1 \equiv -1 + 2U^{n/2} \pmod p$ is a square mod p; that is, $p \equiv 1 \pmod 4$, which proves the second point of Theorem 1.

Remark 5. We do not need the results on the Thue equation $U^3 - 3UV^2 - V^3 = 3$ to prove that if 3 divides an odd integer $U \geq 3$, then $n > 1$ divides the class number of the imaginary quadratic number field $\mathbf{k} = \mathbf{Q}(\sqrt{1 - 4U^n})$, for in that situation we have $\mathbf{k} \neq \mathbf{Q}(\sqrt{-3})$.

References

[AC] N. C. Ankeny and S. Chowla, *On the divisibility of the class number of quadratic fields*, Pacific J. Math. **5** (1955), 321–324. MR0085301 (19:18f)

[BH] Y. Bilu and G. Hanrot, *Solving Thue equations of high degree*, J. Number Theory **60** (1996), 373–392. MR1412969 (97k:11040)

[Co] J. H. E. Cohn, *On the class number of certain imaginary quadratic fields*, Proc. Amer. Math. Soc. **130** (2002), 1275–1277. MR1879947 (2002j:11127)

[DFKPRW] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig and K. Wildanger, *KANT V4*, J. Symbolic Comput. **24** (1997), 267–283. MR1484479 (99g:11150)

[GR] 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. MR0491708 (58:10911)

[Ki] Y. Kishi, *Note on the divisibility of the class number of certain imaginary quadratic fields*, Glasgow Math. J. **51** (2009), 187–191. MR2471686

[Mur] M. Ram Murty, *Exponents of class groups of quadratic fields*, Topics in number theory (University Park, PA, 1997), 229–239, Math. Appl., 467, Kluwer Acad. Publ., Dordrecht, 1999. MR1691322 (2000b:11123)

[So] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*, J. London Math. Soc. (2) **61** (2000), 681–690. MR1766097 (2001i:11128)

Institut de Mathématiques de Luminy, UMR 6206, 163, avenue de Luminy, Case 907, 13288 Marseille Cedex 9, France

E-mail address: loubouti@iml.univ-mrs.fr