THE RAMANUJAN JOURNAL, 7, 449–453, 2003

Congruences for Quadratic Units of Norm −1

RONALD J. EVANS revans@euclid.ucsd.edu
Department of Mathematics, University of California at San Diego, La Jolla, California 92093-0112

PIERRE KAPLAN pierre.kaplan@wanadoo.fr
Département de Mathématiques, Université de Nancy I, Vandoeuvre lès Nancy 54506, France

KENNETH S. WILLIAMS* williams@math.carleton.ca
Centre for Research in Algebra and Number Theory, School of Mathematics and Statistics, Carleton University, Ottawa, Ontario K1S 5B6, Canada

Received October 31, 2000; Accepted February 7, 2001

Abstract. Let $D \equiv 1 \pmod 4$ be a positive integer. Let R be the ring $\{x + y(1+\sqrt{D})/2 \ : x, y \in \mathbb{Z}\}$. Suppose that R contains a unit ϵ of norm -1 as well as an element π of norm 2, and thus an element λ of norm -2. It is not hard to see that $\epsilon \equiv \pm 1 \pmod{\pi^2}$. In this paper we determine ϵ modulo π^3 and modulo λ^3 using only elementary techniques. This determination extends a recent result of Mastropietro, which was proved using class field theory.

Key words: quadratic units of norm -1, quadratic elements of norm ± 2

2000 AMS Mathematics Subject Classification: Primary—11R11, 11R27

1. Introduction

Mastropietro [3, p. 65] has proved the following result.

Proposition. *Let p be a prime with $p \equiv 1 \pmod 8$ for which the real quadratic field $\mathbb{Q}(\sqrt{p})$ contains an integer π of norm 2. The integer π is necessarily of the form $\frac{1}{2}(A + B\sqrt{p})$, where A and B are odd integers; replacing π by $-\pi$, if necessary, we may suppose that $A \equiv -1 \pmod 4$. Let ϵ be a unit of $\mathbb{Q}(\sqrt{p})$ of norm -1. Then*

$$\epsilon \equiv \begin{cases} \pm 1 \pmod{\pi^3}, & \text{if } \pi > 0, \\ \pm 3 \pmod{\pi^3}, & \text{if } \pi < 0. \end{cases}$$

We note that a classical theorem going back to Legendre [2, pp. 64–65] guarantees that the real quadratic field $\mathbb{Q}(\sqrt{p})$ contains units of norm -1 whenever p is a prime $\equiv 1 \pmod 4$. For a more modern reference, see for example [5, pp. 98–99]. We also note that there are primes $p \equiv 1 \pmod 8$ for which $\mathbb{Q}(\sqrt{p})$ does not contain an integer of norm 2,

*Research of the third author was supported by Natural Sciences and Engineering Research Council of Canada grant A-7233.

for example $p = 257$. However, if $\mathbb{Q}(\sqrt{p})$ has class number 1, then it always contains an integer of norm 2, since then 2 splits into a product of prime elements.

An interesting feature of the congruence in the Proposition is that $\epsilon \pmod{\pi^3}$ depends on the sign of π. Mastropietro proved his congruence using class field theory. Recently he asked the first author for a simpler proof. In Section 2, we provide an elementary proof of an extension of Mastropietro's result in which the prime p is replaced by a positive integer $D \equiv 1 \pmod 4$, which is not necessarily squarefree. The proof of our theorem requires nothing deeper than the law of quadratic reciprocity. We prove

Theorem. *Let $D \equiv 1 \pmod 4$ be a positive integer for which the ring $R = \{x + y(1 + \sqrt{D})/2 \ : \ x, y \in \mathbb{Z}\}$ contains a unit ϵ of norm -1 as well as an element π of norm 2, and thus an element λ of norm -2. The elements π and λ must necessarily be of the forms $\pi = \frac{1}{2}(A + B\sqrt{D})$ and $\lambda = \frac{1}{2}(E + F\sqrt{D})$, where A, B, E, and F are odd integers. Then we have the following congruences in R:*

$$\epsilon \equiv \begin{cases} \pm 1 \pmod{\pi^3}, & \text{if } \operatorname{sgn} \pi = (-1)^{(A+1)/2}, \\ \pm 3 \pmod{\pi^3}, & \text{if } \operatorname{sgn} \pi = (-1)^{(A-1)/2}, \end{cases}$$

and

$$\epsilon \equiv \begin{cases} \pm 1 \pmod{\lambda^3}, & \text{if } \operatorname{sgn} \lambda = (-1)^{(F+1)/2}, \\ \pm 3 \pmod{\lambda^3}, & \text{if } \operatorname{sgn} \lambda = (-1)^{(F-1)/2}. \end{cases}$$

The following are twenty examples of composite positive integers $D \equiv 1 \pmod 4$ for which the ring $R = \{x + y(1 + \sqrt{D})/2 \ : \ x, y \in \mathbb{Z}\}$ contains both a unit of norm -1 and an element of norm 2: $D = 17 \cdot 73$, $17 \cdot 113$, $17 \cdot 233$, $17 \cdot 313$, $17 \cdot 673$, $17 \cdot 41 \cdot 233$, $17 \cdot 97 \cdot 433$, $17 \cdot 41 \cdot 89 \cdot 97$, $41 \cdot 137$, $41 \cdot 193$, $41 \cdot 601$, $41 \cdot 113 \cdot 281$, $113 \cdot 409$, $193 \cdot 457$, $401 \cdot 641$, $641 \cdot 937$, $17 \cdot 73^2$, $17 \cdot 41^2 \cdot 113$, $17^2 \cdot 137 \cdot 241$, and $233 \cdot 401^2$. We conjecture that there are infinitely many such D. Dirichlet [1, pp. 656–662; Werke I, pp. 228–234] and Tano [4] have given classes of odd composite squarefree positive integers D for which units of norm -1 exist in $\mathbb{Q}(\sqrt{D})$. For example, if p and q are primes congruent to 1 modulo 4 and $(\frac{p}{q}) = -1$ then there is a unit in $\mathbb{Q}(\sqrt{pq})$ of norm -1. By Dirichlet's theorem on primes in an arithmetic progression, there are infinitely many such pairs p, q.

2. Proof of Theorem

Let $D \equiv 1 \pmod 4$ be a positive integer for which the ring $R = \{x + y(1 + \sqrt{D})/2 \ : \ x, y \in \mathbb{Z}\}$ contains a unit ϵ of norm -1 and an element π of norm 2. As R contains a unit of norm -1, every prime dividing D is congruent to 1 modulo 4. Moreover, as R contains an element of norm 2, each such prime must in fact be congruent to 1 modulo 8. Thus

$$D \equiv 1 \pmod 8. \tag{1}$$

As ϵ is a unit of R of norm -1, we have

$$\epsilon = T + U\sqrt{D}, \tag{2}$$

where T and U are integers such that

$$T^2 - DU^2 = -1, \quad T \equiv 0 \pmod 4, \quad U \equiv 1 \pmod 2. \tag{3}$$

From (3) we deduce that $(T, U) = 1$ and that every prime divisor of U is congruent to 1 modulo 4, so that $\operatorname{sgn} U = (-1)^{(U-1)/2}$. As $|U\sqrt{D}| > |T|$, we have

$$\operatorname{sgn} \epsilon = \operatorname{sgn} U = (-1)^{(U-1)/2}. \tag{4}$$

As π is an element of R of norm 2, we have

$$\pi = \frac{A + B\sqrt{D}}{2}, \tag{5}$$

where A and B are integers such that

$$A^2 - DB^2 = 8, \quad A \equiv B \equiv 1 \pmod 2. \tag{6}$$

From (6) we deduce that $(A, B) = 1$. As $|A| > |B\sqrt{D}|$, we have

$$\operatorname{sgn} \pi = \operatorname{sgn} A. \tag{7}$$

Next

$$\left(\frac{2}{|B|}\right) = \left(\frac{8}{|B|}\right) = \left(\frac{A^2 - DB^2}{|B|}\right) = \left(\frac{A^2}{|B|}\right) = 1,$$

and thus

$$B \equiv \pm 1 \pmod 8. \tag{8}$$

Now let λ be an element of R of norm -2. Then $\lambda = \epsilon\pi$ for some unit ϵ of norm -1 and some element π of norm 2. From (2) and (5) we have

$$\epsilon\pi = \frac{E + F\sqrt{D}}{2}, \tag{9}$$

where the integers E and F are given by

$$E = AT + DBU, \quad F = AU + BT. \tag{10}$$

From (3) and (6) we see that

$$E^2 - DF^2 = -8, \quad E \equiv F \equiv 1 \pmod 2. \tag{11}$$

From (11) we deduce that $(E, F) = 1$. From (10), (3), and (6), we obtain

$$F \equiv AU \equiv AU - (A-1)(U-1) \equiv A + U - 1 \pmod 4. \tag{12}$$

Next, by the law of quadratic reciprocity, we have

$$\left(\frac{A}{D}\right) = \left(\frac{D}{|A|}\right) = \left(\frac{DB^2}{|A|}\right) = \left(\frac{A^2-8}{|A|}\right) = \left(\frac{-8}{|A|}\right) = \left(\frac{-2}{|A|}\right) \tag{13}$$

and

$$\left(\frac{E}{D}\right) = \left(\frac{D}{|E|}\right) = \left(\frac{DF^2}{|E|}\right) = \left(\frac{E^2+8}{|E|}\right) = \left(\frac{8}{|E|}\right) = \left(\frac{2}{|E|}\right). \tag{14}$$

Further, by (6), (8), and (3), we obtain

$$(AU)^2 \equiv (DB^2+8)U^2 \equiv DU^2 + 8 \equiv T^2 + 9 \equiv 9 \pmod{16}$$

so that

$$AU \equiv \pm 3 \pmod 8. \tag{15}$$

Set $T = 2^e T_1$, where T_1 is odd. By the law of quadratic reciprocity, we deduce that

$$\left(\frac{T}{D}\right) = \left(\frac{2^e T_1}{D}\right) = \left(\frac{T_1}{D}\right) = \left(\frac{D}{|T_1|}\right) = \left(\frac{DU^2}{|T_1|}\right) = \left(\frac{T^2+1}{|T_1|}\right) = \left(\frac{1}{|T_1|}\right) = 1. \tag{16}$$

From (10) we have $E \equiv AT \pmod D$, so that appealing to (14), (16), and (13), we obtain

$$\left(\frac{2}{|E|}\right) = \left(\frac{E}{D}\right) = \left(\frac{AT}{D}\right) = \left(\frac{A}{D}\right) = \left(\frac{-2}{|A|}\right).$$

Hence

$$\left(\frac{2}{|EA|}\right) = \left(\frac{-1}{|A|}\right) = (-1)^{(|A|-1)/2} = (\operatorname{sgn} A)(-1)^{(A-1)/2}. \tag{17}$$

By (10), (6), (1), (8), and (15), we have

$$EA = A^2T + DBAU \equiv T + (\pm 1)(\pm 3) \equiv T \pm 3 \pmod 8$$

so that

$$\left(\frac{2}{|EA|}\right) = (-1)^{\frac{T}{4}+1}. \tag{18}$$

From (7), (17), and (18) we obtain

$$\operatorname{sgn} \pi = (-1)^{\frac{A+1}{2}+\frac{T}{4}}. \tag{19}$$

From (4), (19), and (12) we have

$$\operatorname{sgn} \lambda = \operatorname{sgn} \epsilon\pi = (-1)^{\frac{U-1}{2}+\frac{A+1}{2}+\frac{T}{4}} = (-1)^{\frac{F+1}{2}+\frac{T}{4}}. \tag{20}$$

Cubing (5), we obtain

$$\pi^3 = \frac{G + H\sqrt{D}}{2}, \tag{21}$$

where

$$\begin{aligned} 4G &= A^3 + 3AB^2D \equiv A + 3A \equiv 4A \equiv 4 \pmod 8, \\ 4H &= 3A^2B + B^3D \equiv 3B + B \equiv 4B \equiv 4 \pmod 8, \end{aligned}$$

so that $G \equiv H \equiv 1 \pmod 2$. From (21) we have $H\sqrt{D} \equiv -G \pmod{\pi^3}$. Thus, as $\pi^3 \mid 8$, we have using (6)

$$\begin{aligned} \sqrt{D} &\equiv H^2\sqrt{D} \equiv -GH \equiv -\frac{AB}{16}(A^2 + 3B^2D)(3A^2 + B^2D) \\ &\equiv -AB(A^2 - 6)(A^2 - 2) \equiv -AB(1 - 6)(1 - 2) \pmod{\pi^3}, \end{aligned}$$

so that

$$\sqrt{D} \equiv 3AB \pmod{\pi^3}. \tag{22}$$

Hence, by (22), (15), and (8), we obtain

$$U\sqrt{D} \equiv 3(AU)B \equiv 3(\pm 3)(\pm 1) \equiv \pm 1 \pmod{\pi^3},$$

and so

$$\epsilon = T + U\sqrt{D} \equiv T \pm 1 \equiv \begin{cases} \pm 1 \pmod{\pi^3}, & \text{if } T \equiv 0 \pmod 8, \\ \pm 3 \pmod{\pi^3}, & \text{if } T \equiv 4 \pmod 8. \end{cases} \tag{23}$$

The first assertion of our theorem follows from (19) and (23), and the second from (20) and (23).

References

1. P.G.L. Dirichlet, *Einige neue Sätze über unbestimmte Gleichungen*, Abhand. König. Preuss. Akad. Wissen. (1834), 649–664. (Werke I, Chelsea (1969), 221–236.)
2. A.-M. Legendre, *Théorie des Nombres*, vol. I, 4th edition, Albert Blanchard, Paris (1955).
3. M. Mastropietro, "Quadratic forms and relative quadratic extensions," Ph.D. thesis, University of California, San Diego (2000).
4. F. Tano, "Sur quelques théorèmes de Dirichlet," *J. Reine Angew. Math.* **105** (1889), 160–169.
5. A. Weil, *Number Theory: An Approach through History*, Birkhäuser, Boston (1984).