SEMI-ASSOCIATES IN $Z[\sqrt{2}]$ AND PRIMITIVE PYTHAGOREAN TRIPLES*

DELANO P. WEGENER
Central Michigan University, Mount Pleasant, Michigan

1. INTRODUCTION

Waclaw Sierpinski [2, p. 6], [3, p. 94] raised the following question:

SIERPINSKI'S PROBLEM: Are there an infinite number of primitive pythagorean triples with both the hypotenuse and the odd leg equal to a prime?

This question is equivalent to asking for an infinite number of solutions, in primes, to the Diophantine equation $q^2 = 2p - 1$. Other than this simple transformation it seems that no progress has been made toward a solution to Sierpinski's problem.

As a result of his work on Sierpinski's Problem, I. A. Barnett raised the following questions:

QUESTION A: Are there an infinite number of primitive pythagorean triples for which the sum of the legs is a prime?

QUESTION B: Are there an infinite number of primitive pythagorean triples for which the absolute value of the difference of the legs is a prime?

QUESTION C: Are there an infinite number of primitive pythagorean triples for which both the sum of the legs and the absolute value of the difference of the legs are prime?

For a complete discussion and characterization of primitive pythagorean triangles with either the sum or the difference of legs equal to a prime consult [4]. The more interesting aspects of [4] are summarized in the following.

Every prime divisor of either the sum or the difference of the legs of a primitive pythagorean triangle is congruent to ±1 modulo 8. Conversely, if p $\equiv \pm 1 \pmod 8$ *is prime, there is a unique primitive pythagorean triangle with the sum of the legs equal to* p. *However, there are two disjoint infinite sequences of primitive pythagorean triangles, with the difference of the legs equal to* p, *for every triangle in these sequences. Moreover, every triangle with the difference of the legs equal to* p, *is in one of these sequences.*

In Section 2 of this paper, we define "α is a semi-associate of β" for $\alpha, \beta \in Z[\sqrt{2}]$ and present some elementary properties of this concept. These properties are used in Section 3 to show the equivalence of Question C to four questions about primes in $Z[\sqrt{2}]$.

In this paper we use the integral domain $Z[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Z\}$, where Z denotes the usual set of integers. A detailed discussion of this integral domain is available [1, pp. 231–244], but some of the basic facts and some notations are presented in this section.

I will follow the usual custom of referring to elements of $Z[\sqrt{2}]$ as integers and elements of Z as rational integers.

If $\epsilon = 1 + \sqrt{2}$, then the set of units of $Z[\sqrt{2}]$ is precisely the set $\{\pm\epsilon^n \mid n \in Z\}$.

The primes in $Z[\sqrt{2}]$ are all associates of:

(1) $\sqrt{2}$

(2) All rational primes of the form $8k \pm 3$.
These are called primes of the second degree.

(3) All conjugate factors of rational primes of the form $8k \pm 1$.
These are called primes of the first degree.

The following notation and terminology will be used. If $\alpha = a + b\sqrt{2}$, then

*This research is a portion of the author's doctoral dissertation written at Ohio University, Athens, Ohio.

$\bar{a} = a - b\sqrt{2}$ is called the conjugate of a.
$N(a) = a\bar{a}$ is called the norm of a.
$R(a) = a$ is called the rational part of a.
$I(a) = b$ is called the irrational part of a.
$\epsilon = 1 + \sqrt{2}$ is called the fundamental unit in $Z[\sqrt{2}]$.
$\epsilon^{-1} = -1 + \sqrt{2}$ is called the inverse of ϵ.

Each of the properties listed in Lemma 1 is an elementary consequence of the definitions of the symbols involved but are useful in later sections. Proofs can easily be supplied by the reader.

Lemma 1. If a and β are integers, then

$$\overline{a\beta} = \bar{a}\bar{\beta}$$

$$N(a\beta) = N(a)N(\beta), \qquad a + \bar{a} = 2R(a), \qquad a - \bar{a} = 2\sqrt{2}I(a)$$

$$R(a\beta) = R(a)R(\beta) + 2I(a)I(\beta), \qquad I(a\beta) = I(a)R(\beta) + R(a)I(\beta)$$

$$R(a\bar{\beta}) = R(a)R(\beta) - 2I(a)I(\beta), \qquad I(a\bar{\beta}) = R(\beta)I(a) - R(a)I(\beta)$$

$$R(a^2) = R^2(a) + 2I^2(a), \qquad I(a^2) = 2R(a)I(a)$$

$$R(a\epsilon) = R(a) + 2I(a), \qquad I(a\epsilon) = R(a) + I(a)$$

$$R(a\epsilon^{-1}) = 2I(a) - R(a), \qquad I(a\epsilon^{-1}) = R(a) - I(a)$$

$$N(a) = 2I(a)I(a\epsilon^{-1}) - R(a)R(a\epsilon^{-1}), \qquad N(a) = R(a)I(a\epsilon) - R(a\epsilon)I(a).$$

The following lemma summarizes all of the information needed about Pell-type equations.

Lemma 2. If p is a rational prime of the form $8k \pm 1$, the equation $x^2 - 2y^2 = p$ has exactly one solution $x = a$, $y = b$ such that the following two equivalent statements are true:

(i) $$\sqrt{p} < a < \sqrt{2p}$$

(ii) $$0 < b < \sqrt{p/2}.$$

The equation $x^2 - 2y^2 = p$ has infinitely many solutions, all of which are obtained from $(a + b\sqrt{2})\epsilon^{2t}$, where t is any rational integer and $x = a$, $y = b$ is any solution of $x^2 - 2y^2 = p$.
The unique solution which satisfies (i) and (ii) will be called the fundamental solution.

2. SEMI-ASSOCIATES IN $Z[\sqrt{2}]$

Theorem 1. If a and β are integers in $Z[\sqrt{2}]$, then the following are equivalent.

(1) Some associate, call it γ, of β has the same irrational part as a and $\gamma\epsilon$ has the same rational part as a.
(2) There is a rational integer n such that either:
(a) $$I(\beta\epsilon^n) = I(a) \quad \text{and} \quad R(\beta\epsilon^{n+1}) = R(a)$$
or
(b) $$I(-\beta\epsilon^n) = I(a) \quad \text{and} \quad R(-\beta\epsilon^{n+1}) = R(a).$$
(3) β is an associate of $[R(a) - 2I(a)] + I(a)\sqrt{2}$.
(4) β is an associate of $a - 2I(a)$.
(5) $\pm N(\beta) = N(a) + 4I(a)[I(a) - R(a)]$.
(6) $\pm N(\beta) = N(a) - 4I(a)I(a\epsilon^{-1})$.
(7) $N(a) \pm N(\beta) = 4I(a)[R(a) - I(a)]$.
(8) $N(a) \pm N(\beta) = 4I(a)I(a\epsilon^{-1})$.

Proof. It is clear from the characterization of associates in $Z[\sqrt{2}]$ and from Lemma 1 that: (1) $\Leftrightarrow$ (2), (3) $\Leftrightarrow$ (4), (5) $\Leftrightarrow$ (6) $\Leftrightarrow$ (7) $\Leftrightarrow$ (8). To complete the proof we show (1) $\Leftrightarrow$ (3) and (4) $\Leftrightarrow$ (5).

To see that (3) $\Rightarrow$ (1), let $\gamma = [R(a) - 2I(a)] + I(a)\sqrt{2}$ and observe that $I(\gamma) = I(a)$ and $R(\gamma\epsilon) = R(a)$.

To see that (1) $\Rightarrow$ (3), assume β is an associate of γ with $I(\gamma) = I(a)$, and $R(\gamma\epsilon) = R(a)$. Then γ must be of the form $\gamma = r + I(a)\sqrt{2}$ and hence

$$\gamma\epsilon = [r + 2I(a)] + [I(a) + r]\sqrt{2}\,.$$

Now $R(\gamma\epsilon) = R(a)$ implies $r = R(a) - 2I(a)$. Hence

$$\gamma = [R(a) - 2I(a)] + I(a)\sqrt{2}\,.$$

To prove (4) $\Leftrightarrow$ (5), note β is an associate of $a - 2I(a)$ if and only if

$$\pm N(\beta) = N[a - 2I(a)] = [R(a) - 2I(a)]^2 - 2I^2(a) = R^2(a) - 4I(a)R(a) + 4I^2(a) - 2I^2(a)$$
$$= N(a) + 4I(a)[I(a) - R(a)]\,.$$

Definition 1. If a and β are integers in $Z[\sqrt{2}]$ which satisfy any one, and hence all, of the conditions of Theorem 1, then a is called a semi-associate of β.

It is clear that the relation "is a semi-associate of" is not an equivalence relation. The next sequence of theorems characterizes those elements for which the relation is either reflexive, symmetric, or transitive.

Theorem 2. Let a be an integer in $Z[\sqrt{2}]$. a is a semi-associate of itself if and only if

$$R(a)I(a)R(a\epsilon^{-1})I(a\epsilon^{-1}) = 0\,.$$

Proof. The theorem follows easily from the fact that a is a semi-associate of itself if and only if

$$4I(a)I(a\epsilon^{-1}) = N(a) + N(a) = 4I(a)I(a\epsilon^{-1}) - 2R(a)R(a\epsilon^{-1})$$

or

$$4I(a)I(a\epsilon^{-1}) = N(a) - N(a) = 0\,.$$

Corollary. The primes in $Z[\sqrt{2}]$ which are semi-associates of themselves are $\pm\sqrt{2}$, $\pm\epsilon\sqrt{2}$, $\pm p$, $\pm\epsilon p$, where $p\epsilon\{p \mid p$ is a rational prime of the form $8k \pm 3\}$.

Proof. That each of the primes listed is a semi-associate of itself follows directly from the theorem. To see that these are the only possibilities, consider the four cases:

(i) $R(a) = 0$

(ii) $I(a) = 0$

(iii) $R(a) - I(a) = I(a\epsilon^{-1}) = 0.$

(iv) $2I(a) - R(a) = R(a\epsilon^{-1}) = 0.$

Theorem 3. Two integers a and β are semi-associates of each other if and only if one of the following four pairs of conditions is true:

(i) $I(a)I(a\epsilon^{-1}) = I(\beta)I(\beta\epsilon^{-1})$, $\quad R(a)R(a\epsilon^{-1}) = -R(\beta)R(\beta\epsilon^{-1})$

(ii) $I(a)I(a\epsilon^{-1}) = -I(\beta)I(\beta\epsilon^{-1})$, $\quad R(a)R(a\epsilon^{-1}) = R(\beta)R(\beta\epsilon^{-1})$

(iii) $2I(a)I(a\epsilon^{-1}) = -R(\beta)R(\beta\epsilon^{-1})$, $\quad R(a)R(a\epsilon^{-1}) = 2I(\beta)I(\beta\epsilon^{-1})$

(iv) $2I(a)I(a\epsilon^{-1}) = R(\beta)R(\beta\epsilon^{-1})$, $\quad R(a)R(a\epsilon^{-1}) = -2I(\beta)I(\beta\epsilon^{-1})$.

Proof. If a is a semi-associate of β and simultaneously β is a semi-associate of a, then by Theorem 1, part 8,

$$N(a) \pm N(\beta) = 4I(a)I(a\epsilon^{-1}) \quad \text{and} \quad N(\beta) \pm N(a) = 4I(\beta)I(\beta\epsilon^{-1})\,.$$

This leads to the following four cases:

Case 1. $N(a) + N(\beta) = 4I(a)I(a\epsilon^{-1})$, $\quad N(a) + N(\beta) = 4I(\beta)I(\beta\epsilon^{-1})$.

Case 2. $N(a) - N(\beta) = 4I(a)I(a\epsilon^{-1})$, $\quad N(\beta) - N(a) = 4I(\beta)I(\beta\epsilon^{-1})$.

Case 3. $N(a) + N(\beta) = 4I(a)I(a\epsilon^{-1})$, $\quad N(\beta) - N(a) = 4I(\beta)I(\beta\epsilon^{-1})$.

Case 4. $N(a) - N(\beta) = 4I(a)I(a\epsilon^{-1})$, $\quad N(\beta) + N(a) = 4I(\beta)I(\beta\epsilon^{-1})$.

In Case 1 it is clear that

$$I(a)I(a\epsilon^{-1}) = I(\beta)I(\beta\epsilon^{-1})$$

and then by Lemma 1,

$$4I(a)I(a\epsilon^{-1}) = N(a) + N(\beta) = -R(a)R(a\epsilon^{-1}) + 2I(a)I(a\epsilon^{-1}) - R(\beta)R(\beta\epsilon^{-1}) + 2I(\beta)I(\beta\epsilon^{-1})$$
$$= -R(a)R(a\epsilon^{-1}) - R(\beta)R(\beta\epsilon^{-1}) + 4I(a)I(a\epsilon^{-1}).$$

It now follows that

$$R(a)R(a\epsilon^{-1}) = -R(\beta)R(\beta\epsilon^{-1}).$$

Conversely if

$$I(a)I(a\epsilon^{-1}) = I(\beta)I(\beta\epsilon^{-1}) \quad \text{and} \quad R(a)R(a\epsilon^{-1}) = -R(\beta)R(\beta\epsilon^{-1})$$

then by Lemma 1,

$$N(a) + N(\beta) = -R(a)R(a\epsilon^{-1}) + 2I(a)I(a\epsilon^{-1}) - R(\beta)R(\beta\epsilon^{-1}) + 2I(\beta)I(\beta\epsilon^{-1}) = 4I(a)I(a\epsilon^{-1})$$
$$= 4I(\beta)I(\beta\epsilon^{-1}).$$

Thus by Theorem 1, a and β are semi-associates of each other. In Case 2, it is clear that

$$I(a)I(a\epsilon^{-1}) = -I(\beta)I(\beta\epsilon^{-1})$$

and as in Case 1, Lemma 1 implies that

$$R(a)R(a\epsilon^{-1}) = R(\beta)R(\beta\epsilon^{-1}).$$

The converse again follows from Lemma 1. In Case 3, addition of the two equalities yields

$$N(\beta) = 2I(a)I(a\epsilon^{-1}) + 2I(\beta)I(\beta\epsilon^{-1})$$

and then by Lemma 1,

$$-R(\beta)R(\beta\epsilon^{-1}) + 2I(\beta)I(\beta\epsilon^{-1}) = N(\beta) = 2I(a)I(a\epsilon^{-1}) + 2I(\beta)I(\beta\epsilon^{-1}).$$

Thus

$$2I(a)I(a\epsilon^{-1}) = -R(\beta)R(\beta\epsilon^{-1}).$$

On the other hand if the second equality is subtracted from the first and Lemma 1 is used we get

$$-R(a)R(a\epsilon^{-1}) + 2I(a)I(a\epsilon^{-1}) = N(a) = 2I(a)I(a\epsilon^{-1}) - 2I(\beta)I(\beta\epsilon^{-1}).$$

Thus

$$R(a)R(a\epsilon^{-1}) = 2I(\beta)I(\beta\epsilon^{-1}),$$

Conversely if both conditions in (iii) are true, then direct computation, using Lemma 1, shows

$$N(a) + N(\beta) = 4I(a)I(a\epsilon^{-1}) \quad \text{and} \quad N(\beta) - N(a) = 4I(\beta)I(\beta\epsilon^{-1})$$

and hence a and β are semi-associates of each other. In Case 4, addition of the two equalities and Lemma 1 yields

$$R(a)R(a\epsilon^{-1}) = -2I(\beta)I(\beta\epsilon^{-1}).$$

Subtraction of the first equality from the second and Lemma 1 yields

$$2I(a)I(a\epsilon^{-1}) = R(\beta)R(\beta\epsilon^{-1}).$$

The converse is proved by direct computation as indicated in Case 3. This completes the proof.

Integers a and β which are semi-associates of each other may also be characterized in terms of norms and rational parts of integers.

Theorem 4. Two integers a and β are semi-associates of each other if and only if one of the following four pairs of conditions is true:

(i) $N(a) = R(\beta^2\epsilon^{-1})$, $N(\beta) = R(a^2\epsilon^{-1})$

(ii) $N(a) = -R(\beta^2\epsilon^{-1})$, $N(\beta) = -R(a^2\epsilon^{-1})$

(iii) $N(a) = -R(\beta^2\epsilon^{-1})$, $N(\beta) = R(a^2\epsilon^{-1})$

(iv) $N(a) = R(\beta^2\epsilon^{-1})$, $N(\beta) = -R(a^2\epsilon^{-1})$.

Proof. If the conditions in part (i) of Theorem 3 are true, then from Lemma 1,

$$R(\alpha^2\epsilon^{-1}) = R(\alpha)R(\alpha\epsilon^{-1}) + 2I(\alpha)I(\alpha\epsilon^{-1}),$$

and hence,

$$N(\beta) = 2I(\beta)I(\beta\epsilon^{-1}) - R(\beta)R(\beta\epsilon^{-1}) = R(\alpha)R(\alpha\epsilon^{-1}) + 2I(\alpha)I(\alpha\epsilon^{-1}) = R(\alpha^2\epsilon^{-1}).$$

Similarly

$$N(\alpha) = R(\beta^2\epsilon^{-1}).$$

Conversely, if

$$N(\beta) = R(\alpha^2\epsilon^{-1}) \quad \text{and} \quad N(\alpha) = R(\beta^2\epsilon^{-1}),$$

then

$$2I(\beta)I(\beta\epsilon^{-1}) - R(\beta)R(\beta\epsilon^{-1}) = N(\beta) = R(\alpha^2\epsilon^{-1}) = 2I(\alpha)I(\alpha\epsilon^{-1}) + R(\alpha)R(\alpha\epsilon^{-1}),$$

and

$$2I(\alpha)I(\alpha\epsilon^{-1}) - R(\alpha)R(\alpha\epsilon^{-1}) = N(\alpha) = R(\beta^2\epsilon^{-1}) = 2I(\beta)I(\beta\epsilon^{-1}) + R(\beta)R(\beta\epsilon^{-1}).$$

Addition of these two equalities yields

$$I(\alpha)I(\alpha\epsilon^{-1}) = I(\beta)I(\beta\epsilon^{-1})$$

and subtraction yields

$$R(\alpha)R(\alpha\epsilon^{-1}) = -R(\beta)R(\beta\epsilon^{-1}).$$

Thus condition (i) of Theorem 3 is true and α and β are semi-associates of each other. Similar arguments show that conditions (ii), (iii), and (iv) of this theorem are equivalent to conditions (ii), (iii), and (iv) of Theorem 3 and the proof is complete.

The property of transitivity for the relation "is a semi-associate of" is closely related to reflexivity. This relation is expressed in Theorem 5.

Theorem 5. If α, β, and γ are integers in $Z[\sqrt{2}]$ such that α is a semi-associate of β and β is a semi-associate of γ, then α is a semi-associate of γ if and only if β is a semi-associate of itself.

Proof. If α is a semi-associate of β and β is a semi-associate of γ and itself, then β and γ are associates and hence α is a semi-associate of γ. Conversely if β is a semi-associate of γ and α is a semi-associate of both β and γ, then β and γ are associates and thus β is an associate of $\beta - 2I(\beta)$ because γ is. Hence β is a semi-associate of itself.

The following results will be particularly useful in the next section.

Lemma 3.

$$R(\beta^2\epsilon^{2k+1}) = N[\beta\epsilon^k + 2I(\beta\epsilon^k)].$$

Proof.

$$\begin{aligned} R(\beta^2\epsilon^{2k+1}) &= R^2(\beta\epsilon^k) + 4R(\beta\epsilon^k)I(\beta\epsilon^k) + 2I(\beta\epsilon^k) \\ &= [R(\beta\epsilon^k) + 2I(\beta\epsilon^k)]^2 - 2I^2(\beta\epsilon^k) = N[\beta\epsilon^k + 2I(\beta\epsilon^k)]. \end{aligned}$$

Theorem 6. If α is a semi-associate of β, then

$$N(\alpha) = R(\beta^2\epsilon^{2k+1})$$

for some rational integer k.

Proof. Since α is a semi-associate of β, it follows from Theorem 1, that there is a rational integer k such that exactly one of the following cases is true:

Case 1. $I(\beta\epsilon^k) = I(\alpha)$ and $R(\beta\epsilon^k) = R(\alpha) - 2I(\alpha)$.

Case 2. $I(-\beta\epsilon^k) = I(\alpha)$ and $R(-\beta\epsilon^k) = R(\alpha) - 2I(\alpha)$.

In Case 1 we have

$$\begin{aligned} R(\beta^2\epsilon^{2k+1}) &= R(\beta^2\epsilon^{2k}) + 2I(\beta^2\epsilon^{2k}) = R^2(\beta\epsilon^k) + 2I^2(\beta\epsilon^k) + 4R(\beta\epsilon^k)I(\beta\epsilon^k) \\ &= [R(\alpha) - 2I(\alpha)]^2 + 2I^2(\alpha) + 4I(\alpha)[R(\alpha) - 2I(\alpha)] \\ &= R^2(\alpha) - 2I^2(\alpha) = N(\alpha). \end{aligned}$$

In Case 2 note that

$$I(-\eta) = -I(\eta) \quad \text{and} \quad -R(\eta) = R(-\eta)$$

for any $\eta \in Z[\sqrt{2}]$ and then

$$\begin{aligned} R(\beta^2\epsilon^{2k+1}) &= R(\beta^2\epsilon^{2k}) + 2I(\beta^2\epsilon^{2k}) = R^2(\beta\epsilon^k) + 2I^2(\beta\epsilon^k) + 4R(\beta\epsilon^k)I(\beta\epsilon^k) \\ &= R^2(-\beta\epsilon^k) + 2I^2(-\beta\epsilon^k) + 4R(-\beta\epsilon^k)I(-\beta\epsilon^k) \\ &= [R(\alpha) - 2I(\alpha)]^2 + 2I^2(\alpha) + 4I(\alpha)[R(\alpha) - 2I(\alpha)] \\ &= R^2(\alpha) - 2I^2(\alpha) = N(\alpha) . \end{aligned}$$

Theorem 6 gives a necessary condition for one integer to be a semi-associate of another integer. This condition does not seem to be sufficient, but a partial result in this direction is given in Theorem 7.

Theorem 7. If α is a prime and

$$N(\alpha) = R(\beta^2\epsilon^{2k+1})$$

for some rational integer k, then some associate of α or some associate of $\bar{\alpha}$ is a semi-associate of β.

Proof. If

$$N(\alpha) = R(\beta^2\epsilon^{2k+1}),$$

then by Lemma 3

$$N(\alpha) = N[\beta\epsilon^k + 2I(\beta\epsilon^k)]$$

so that either α or $\bar{\alpha}$ is an associate of

$$\beta\epsilon^k + 2I(\beta\epsilon^k).$$

Consider the case where α is an associate of

$$\beta\epsilon^k + 2I(\beta\epsilon^k).$$

Then there is a rational integer t such that

$$\pm\alpha\epsilon^t = \beta\epsilon^k + 2I(\beta\epsilon^k).$$

Hence

$$\beta\epsilon^k = \beta\epsilon^k + 2I(\beta\epsilon^k) - 2I(\beta\epsilon^k) = \pm\alpha\epsilon^t - 2I(\beta\epsilon^k) = \pm\alpha\epsilon^t - 2I(\pm\alpha\epsilon^t).$$

Thus β is an associate of

$$\pm\alpha\epsilon^t - 2I(\pm\alpha\epsilon^t)$$

and hence $\pm\alpha\epsilon^t$ is a semi-associate of β. The remaining case follows in a similar fashion.

3. EQUIVALENT FORMS OF QUESTION C

The term "generators" of a primitive pythagorean triple will mean the quantities m and n in the familiar formulae:

$$x = 2mn, \qquad y = m^2 - n^2, \qquad z = m^2 + n^2,$$

where m and n are of opposite parity, $(m,n) = 1$, and $m > n$.

Theorem 8. Let p and q be rational primes of the form $8k \pm 1$ (not necessarily of the same form). Let $u = a$, $v = b$ be the fundamental solution of $u^2 - 2v^2 = p$, and let $\alpha = a + b\sqrt{2}$. Let $u = c$, $v = d$ be the fundamental solution of $u^2 - 2v^2 = q$ and let $\beta = c + d\sqrt{2}$. If (x,y,z) is a primitive pythagorean triangle such that $x + y = p$ and $|x - y| = q$, then α is a semi-associate of β or $\bar{\beta}$.

Proof. Let m and n be the generators of (x,y,z). Since

$$p = x + y = (m+n)^2 - 2n^2 > (2n)^2 - 2n^2 = 2n^2$$

it follows that $u = m + n$ and $v = n$ is the fundamental solution of $u^2 - 2v^2 = p$. Hence $a = m + n$ and $b = n$. Now note that

$$N(\beta) = q = |y - x| = |(m-n)^2 - 2n^2| = |N[(m-n) + n\sqrt{2}]| = |N[\alpha - 2I(\alpha)]| .$$

Since β is prime it follows that β or $\overline{\beta}$ is an associate of $\alpha - 2I(\alpha)$ and hence α is a semi-associate of β or $\overline{\beta}$.

Theorem 9. Let α and β be primes of the first degree in $Z[\sqrt{2}]$. Let p and q be the rational primes such that $N(\alpha) = p$ and $N(\beta) = q$. If α is a semi-associate of β, then there is a primitive pythagorean triangle (x,y,z) such that $x + y = p$ and $|x - y| = q$.

Proof. Let $\alpha = a + b\sqrt{2}$ and $\beta = c + d\sqrt{2}$. Let $m = a - b$ and $n = b$. Then m and n generate a primitive pythagorean triangle (x,y,z) such that

$$x + y = (m + n)^2 - 2n^2 = a^2 - 2b^2 = N(\alpha) = p.$$

Since

$$\alpha = a + b\sqrt{2} = (m + n) + n\sqrt{2}$$

is a semi-associate of $\beta = c + d\sqrt{2}$, there is a rational integer n_0 such that the conditions in one of the following cases is true:

Case 1. $\beta\epsilon^{n_0} = r + n\sqrt{2}$ and $\beta\epsilon^{n_0+1} = (m + n) + s\sqrt{2}$,

where r and s are rational integers.

Case 2. $\beta(-\epsilon^{n_0}) = r + n\sqrt{2}$ and $\beta(-\epsilon^{n_0+1}) = (m + n) + s\sqrt{2}$,

where r and s are rational integers.

In Case 1 we have

$$(m + n) + s\sqrt{2} = \beta\epsilon^{n_0+1} = (r + n\sqrt{2})\epsilon = (r + 2n) + (r + n)\sqrt{2}.$$

Comparing rational parts yields $r = m - n$. Thus

$$\beta\epsilon^{n_0} = (m - n) + n\sqrt{2}.$$

Now we have

$$q = N(\beta) = \pm N(\beta\epsilon^{n_0}) = \pm N[(m - n) + n\sqrt{2}] = \pm[(m - n)^2 - 2n^2] = \pm[(m + n)^2 - 2m^2] = \pm(y - x).$$

Hence, in this case, $|x - y| = q$. In Case 2 we have

$$(m + n) + s\sqrt{2} = (r + n\sqrt{2})\epsilon = (r + 2n) + (r + n)\sqrt{2},$$

and as before we conclude $q = |x - y|$.

Combining the results of Theorems 1, 8, and 9 yields the following theorem.

Theorem 10. The following questions are each equivalent to Question C.

QUESTION D: Are there infinitely many pairs of primes of the first degree in $Z[\sqrt{2}]$ such that one member of the pair is a semi-associate of the other member of the pair?

QUESTION E: Are there infinitely many pairs α and $\alpha - 2I(\alpha)$, of primes of the first degree in $Z[\sqrt{2}]$?

QUESTION F: Are there infinitely many pairs (α,β) of primes of the first degree in $Z[\sqrt{2}]$ such that either

$$N(\alpha) + N(\beta) = 4I(\alpha)I(\alpha\epsilon^{-1}) \quad \text{or} \quad N(\alpha) - N(\beta) = 4I(\alpha)I(\alpha\epsilon^{-1})?$$

Combining the results of Theorems 6, 7, and 10 yields the final theorem.

Theorem 11. Questions C, D, E, and F are all equivalent to:

QUESTION G: Are there infinitely many pairs (α,β) of primes of the first degree in $Z[\sqrt{2}]$ such that

$$N(\alpha) = R(\beta^2\epsilon^{2k+1})$$

for some rational integer k, depending on α and β?

REFERENCES

1. L. W. Reid, *The Elements of the Theory of Algebraic Numbers,* Macmillan, New York, New York, 1910.
2. W. Sierpinski, *Pythagorean Triangles,* Scripta Mathematica Studies, New York, 1962.
3. W. Sierpinski, *A Selection of Problems in the Theory of Numbers,* Macmillan, New York, 1964.
4. D.P. Wegener, "Primitive Pythagorean Triples with Sum or Difference of Legs equal to a Prime," *The Fibonacci Quarterly,* Vol. 13, No. 3 (Oct. 1975), pp. 263–277.

★★★★★★★