Pythagorean Triples Over Gaussian Integers

Cheranoot Somboonkulavudi

Department of Mathematics, Faculty of Science
Chulalongkorn University
Bangkok 10330, Thailand
rung_rung@hotmail.com

Ajchara Harnchoowong

Department of Mathematics, Faculty of Science
Chulalongkorn University
Bangkok 10330, Thailand
Ajchara.h@chula.ac.th

Abstract

This paper investigates the unique factorization of primitive Pythagorean triples over the Gaussian integers. Moreover, we show the isomorphisms between the groups of Pythagorean triples with different operations and the multiplicative group of the quotient field of Gaussian integers.

Mathematics Subject Classification: 11R04, 11R27

Keywords: free abelian group, gaussian integer, pythagorean triple, unique factorization

1 Introduction

Let $K$ be a number field with ring of integers $R$. A triple $(a, b, c)$ of elements of $R$ is said to be a Pythagorean triple if $a^2 + b^2 = c^2$. For $R = \mathbb{Z}$, E. Eckert [3] defined an operation, addition, by $(a_1, b_1, c_1) + (a_2, b_2, c_2) = (a_1a_2 - b_1b_2, a_1b_2 + b_1a_2, c_1c_2)$ so that the set of Pythagorean triples of natural numbers and $(1, 0, 1)$ with + is a free abelian group. P. Zanardo and U. Zannier [6] generalized the domain from $\mathbb{Z}$ to any ring of integers $R$ such that $i \not\in R$. R. Beauregard and E. Suryanarayan [1] considered the set of Pythagorean triples over $\mathbb{Z}$ and defined * by $(a_1, b_1, c_1) * (a_2, b_2, c_2) = (a_1a_2, b_1c_2 + b_2c_1, b_1b_2 + c_1c_2)$. The well-known

---

1Supported by Chulalongkorn University Graduate Scholarship to Commemorate the 72nd Anniversary of His Majesty King Bhumibol Adulyadej
representation of Pythagorean triples in Number Theory resulted in properties
and a unique factorization theorem of primitive Pythagorean triples. The set
of equivalence classes of Pythagorean triples is a free abelian group which is
isomorphic to the multiplicative group of positive rationals.

N. Sexauer [5] investigated solutions of the equation \(x^2 + y^2 = z^2\) on unique
factorization domains satisfying some hypotheses. Later, K. Kubota [4] char-
acterized Pythagorean triples in an arbitrary unique factorization domain.
Where \(R\) is the Gaussian integers, James T. Cross [2] displayed a method
for generating all Pythagorean triples. Each equivalence class of primitive
Pythagorean triples is mapped from a certain pair of Gaussian integers.

Inspired by R. Beauregard and E. Suryanarayan's work, this paper de-
scribed the unique factorization of primitive Pythagorean triples when
\(R\) is

\[\mathbb{Z}[i]\]

and its quotient group is free abelian. In Gaussian integers, \(i = \sqrt{-1}\) comes in handy when we show the relation between
two operations. The last theorem describes that the group of Pythagorean
triples whose first components are non-zero with operation \(*\) is isomorphic to
the group of Pythagorean triples whose third components are non-zero with
the operation \(+\) defined above.

2 The Semigroup of Pythagorean Triples Over
Gaussian Integers

Let \(PT\) be the set of all Pythagorean triples in the ring of Gaussian integers
where their first components are non-zero; i.e.,

\[PT = \{(a, b, c) \mid a, b, c \in \mathbb{Z}[i] \text{ with } a \neq 0; a^2 + b^2 = c^2\}.
\]

Define the operation \(*\) on \(PT\) by

\[(a_1, b_1, c_1) * (a_2, b_2, c_2) = (a_1a_2, b_1c_2 + b_2c_1, b_1b_2 + c_1c_2).\]  \hspace{1cm} (1)

Proposition 2.1. The set \(PT\) under the operation \(*\) is a commutative
monoid with the identity element \((1, 0, 1)\).

Proof. The proof is straightforward and left to the reader. \(\Box\)

K. Kubota determined the representation of Pythagorean triples in a unique
factorization domain [4]. We applied the theorem to the ring of the Gaussian
integers.

Proposition 2.2. If \((a, b, c) \in PT\), then there are \(f, u, v, d \in \mathbb{Z}[i]\) where \(d\)
is a factor of 2 relatively prime to \(f\) and \(d \mid u^2 \pm v^2\) such that

\[a = \frac{2fuv}{d}, \quad b = \frac{f(u^2 - v^2)}{d}, \quad \text{and} \quad c = \frac{f(u^2 + v^2)}{d}. \]  \hspace{1cm} (2)
Definition 2.3. A Pythagorean triple $(a, b, c)$ is said to be primitive if the components $a, b, c$ have no common divisor.

Corollary 2.4. If $(a, b, c) \in PT$ is primitive, then there exist $u, v, d \in \mathbb{Z}[i]$ where $d$ is a factor of 2 and $d \mid u^2 + v^2$ such that

$$a = \frac{2uv}{d}, \quad b = \frac{u^2 - v^2}{d}, \quad \text{and} \quad c = \frac{u^2 + v^2}{d}. \quad (3)$$

Proof. From Proposition 2.2, if $f$ is not a unit, then $(a, b, c)$ is not primitive. □

Parity makes things much easier in $\mathbb{Z}$. James T. Cross use $\delta := 1 + i$ to define ”even” and ”odd” Gaussian integers and gave a proof of the following lemma [2].

Lemma 2.5. $\mathbb{Z}[i]/<\delta> = \{[0], [1]\}$.

Hence $[0]$ and $[1]$ are the residue classes of 0 and 1 in $\mathbb{Z}[i]/<\delta>$, respectively.

Definition 2.6. Let $a$ be a Gaussian integer. We say that $a$ is even or odd according as $a$ is in the residue class determined by 0 or 1.

It follows that all elementary properties of even and oddness hold. For example, the sum of an even Gaussian integer and an odd one is odd.

Lemma 2.7. If $(a, b, c) \in PT$ is primitive, then only one of $a, b, c$ is even and the others are odd.

Proof. Suppose that two of $a, b, c$ are even. Since $a^2 + b^2 = c^2$, all $a, b, c$ are even. This contradicts the fact that $(a, b, c)$ is primitive. □

A significant difference between the set of integers and Gaussian integers is $i$. This number is the key to the next lemma which plays important role in several following theorems. The proof is straightforward.

Lemma 2.8. $(a, b, c) \in PT$ if and only if $(c, bi, a) \in PT$.

The notation $a \sim b$ will be used when $a$ and $b$ are associates. Note that if $d \mid 2$, then $d \sim 1, \delta$ or $\delta^2$.

Proposition 2.9. For each primitive triple $(a, b, c)$ in $PT$, either $a, b$ or $c$ is a multiple of $\delta^3$. 
Proof. By Lemma 2.7, only one of $a, b, c$ is even and the others are odd. If $a$ is even, by Corollary 2.4, there exist Gaussian integers $u, v, d$ where $d \mid 2$ and $d \mid u^2 + v^2$ such that

$$a = \frac{2uv}{d}, \quad b = \frac{u^2 - v^2}{d}, \quad \text{and} \quad c = \frac{u^2 + v^2}{d}.$$  

Case1 : $u$ is even and $v$ is odd. Then $u^2 - v^2$ is odd. Since $b$ is odd, we have $d \sim 1$. Hence $a \sim 2uv$ and thus $a$ is divisible by $\delta^3$.

Case2 : $u$ is odd and $v$ is even. This is similar to the above case.

Case3 : $u$ and $v$ are odd. Both $u - v$ and $u + v$ are divisible by $\delta$. Therefore, $2 \mid u^2 - v^2$. Since $b$ is odd, it follows that $d \sim 2$ and $a \sim uv$. Hence $a$ is odd, a contradiction.

Case4 : $u$ and $v$ are even. If $\delta^2 \mid u$ or $\delta^2 \mid v$, then $a$ is divisible by $\delta^3$ and we are done. Suppose that $\delta^2 \nmid u$ and $\delta^2 \nmid v$. Thus $u = \delta u_1$ and $v = \delta v_1$ where $u_1, v_1$ are odd Gaussian integers. Since $b = (u^2 - v^2)/d = \delta^2(u_1^2 - v_1^2)/d$ and $u_1^2 - v_1^2$ is even, $b$ is even. This is a contradiction.

For the case that $b$ is even, we can prove in a similar way. When $c$ is even by Lemma 2.8, $(c, bi, a) \in PT$ and the above proof shows that $c$ is divisible by $\delta^3$.

\[\square\]

From Proposition 2.9 and Lemma 2.7, there are no Gaussian integers $b_1, b_2, c_1, c_2$ such that $(\delta, b_1, c_1)$ and $(2, b_2, c_2)$ are primitive. However, every odd prime appears in specific forms of primitive Pythagorean triples.

Proposition 2.10. Let $p$ be an odd prime in the Gaussian integers (i.e., $p \sim \delta$). If $p$ occurs as a component of a primitive Pythagorean triple in $PT$, then it must be one of the following forms:

(i) $(p, \pm \frac{p^2 - 1}{2}, \pm \frac{p^2 + 1}{2})$ and $(p, \pm \frac{p^2 + 1}{2}i, \pm \frac{p^2 - 1}{2}i)$

(ii) $(\pm \frac{p^2 - 1}{2}, p, \pm \frac{p^2 + 1}{2})$ and $(\pm \frac{p^2 + 1}{2}i, p, \pm \frac{p^2 - 1}{2}i)$

(iii) $(\pm \frac{p^2 + 1}{2}, \pm \frac{p^2 - 1}{2}i, p)$ and $(\pm \frac{p^2 - 1}{2}i, \pm \frac{p^2 + 1}{2}, p)$.

Proof. It is easy to verify that each triple listed is an element in $PT$. First we will show that case (i) is the only way in which $p$ can occur as the first component of a primitive Pythagorean triple. Let $(p, b, c) \in PT$. By Corollary 2.4, there exist Gaussian integers $u, v, d$ where $d \mid 2$ and $d \mid u^2 + v^2$ such that

$$p = \frac{2uv}{d}, \quad b = \frac{u^2 - v^2}{d}, \quad \text{and} \quad c = \frac{u^2 + v^2}{d}.$$  

Since $p$ is odd, $p \sim 2/d$. Therefore, $p \sim u$ or $p \sim v$. If $p \sim u$, then $v \sim 1$ and $d$ follows from $p = 2uv/d$. It can be seen that there exist exactly 16 combinations
that satisfy the conditions that $p \sim u$ and $v \sim 1$. Upon substituting each of these combinations into the formulas for $b$ and $c$, we obtain 4 possible forms as follows: $(p, (p^2 - 1)/2, (p^2 + 1)/2)$, $(p, -(p^2 - 1)/2, -(p^2 + 1)/2)$, $(p, (p^2 + 1)i/2, (p^2 - 1)i/2)$ and $(p, -(p^2 + 1)i/2, -(p^2 - 1)i/2)$. If $p \sim v$, then $u \sim 1$. Substituting the 16 combinations that satisfy the condition into the formulas given in Corollary 2.4, we obtain 4 formulas where each of the middle components has the different sign from the 4 previous formulas. Case (ii) can be proved similarly and case (iii) follows from Lemma 2.8.

Since each Gaussian integer has the unique factorization up to units, this fact effects the unique factorization of each Pythagorean triple. We then introduce units and irreducible elements in PT.

**Definition 2.11.** $(a, b, c) \in \text{PT}$ is called a unit if there exists $(d, e, f) \in \text{PT}$ such that $(a, b, c) \ast (d, e, f) = (1, 0, 1)$.

**Lemma 2.12.** All units in PT are $(\pm 1, 0, \pm 1)$, $(\pm 1, \pm i, 0)$, $(\pm i, 0, \pm i)$ and $(\pm i, \pm 1, 0)$.

**Proof.** If $(1, b, c) \in \text{PT}$, then there exist $u, v, d \in \mathbb{Z}[i]$ where $d \mid 2$ and $d \mid u^2 + v^2$ such that

$$1 = \frac{2uv}{d}, \quad b = \frac{u^2 - v^2}{d}, \quad \text{and} \quad c = \frac{u^2 + v^2}{d}$$

by Corollary 2.4. This implies that $d \sim 2$, $u \sim 1$, $v \sim 1$ and all triples satisfying these conditions are $(1, 0, \pm 1)$ and $(1, \pm i, 0)$. Since the first component of a unit in PT must associate 1, we are done.

**Definition 2.13.** Let $(a, b, c), (d, e, f) \in \text{PT}$. If there exists a unit $(x, y, z) \in \text{PT}$ such that $(a, b, c) = (d, e, f) \ast (x, y, z)$, we say that $(a, b, c)$ associates $(d, e, f)$ denoted by $(a, b, c) \approx (d, e, f)$. For example, $(3, 4, 5) \approx (3, 5i, 4i)$ since $(3, 5i, 4i) = (3, 4, 5) \ast (1, i, 0)$.

**Definition 2.14.** A non-unit $(a, b, c) \in \text{PT}$ is said to be irreducible provided that: whenever $(a, b, c) = (u, v, w) \ast (x, y, z)$ we will have $(u, v, w)$ or $(x, y, z)$ is a unit. For example, $(1 + 2i, -2 + 2i, -1 + 2i)$ is irreducible but $(12, 5, 13) = (3, 4, 5) \ast (4, -3, 5)$ is not. Furthermore, every triple in case (i) of Proposition 2.10 is irreducible because the prime $p$ cannot be factored.

**Proposition 2.15.** For each positive integer $k \geq 3$, $\delta^k$ occurs as the first component of a primitive Pythagorean triple in PT as follows and in no other way: $(\delta^k, \pm(\delta^{2k-4} + 1), \pm(\delta^{2k-4} - 1))$ and $(\delta^k, \pm(\delta^{2k-4} - 1)i, \pm(\delta^{2k-4} + 1)i)$. Moreover, these triples are irreducible.

**Proof.** Let $(\delta^k, b, c) \in \text{PT}$ be primitive. By Lemma 2.7, $b$ and $c$ must be odd. Then

$$\delta^k = \frac{2uv}{d}, \quad b = \frac{u^2 - v^2}{d}, \quad \text{and} \quad c = \frac{u^2 + v^2}{d}$$
for some Gaussian integers $u, v, d$ where $d \mid 2$ and $d \mid u^2 \pm v^2$ by Corollary 2.4. Case 1: $u$ is even and $v$ is odd. Then $u^2 - v^2$ is odd. Since $b$ is odd, $d \sim 1$ and $\delta^k \sim 2uv$. Hence $v \sim 1$ and $u \sim \delta^{k-2}$. These conditions give rise to 4 possible forms as follows: $(\delta^k, \delta^2 - k - 4 - 1, \delta^2 - k - 4 - 1)$, $(\delta^k, -\delta^2 - k - 4 - 1, -\delta^2 - k - 4 - 1)$, $(\delta^k, (\delta^2 - k - 4 - 1)i, (\delta^2 - k - 4 + 1)i)$ and $(\delta^k, -\delta^2 - k - 4 - 1)i, -\delta^2 - k - 4 + 1)i$.

Case 2: $u$ is odd and $v$ is even. Similarly, $d \sim 1, u \sim 1$ and $v \sim \delta^{k-2}$. We obtain another 4 possible forms where the middle components have different signs from the previous case: $(\delta^k, -\delta^2 - k - 4 + 1, \delta^2 - k - 4 - 1)$, $(\delta^k, \delta^2 - k - 4 + 1, -\delta^2 - k - 4 - 1)$, $(\delta^k, (\delta^2 - k - 4 - 1)i, (\delta^2 - k - 4 + 1)i)$ and $(\delta^k, (\delta^2 - k - 4 - 1)i, -\delta^2 - k - 4 + 1)i$.

Case 3: $u$ and $v$ are odd. Since $\delta^k = 2uv/d$ and $k \geq 3$, this is a contradiction. Case 4: $u$ and $v$ are even. Since $b = (u^2 - v^2)/d$ is odd, $d \sim 2$ and $u, v$ cannot be both divisible by $\delta^2$. If $u \sim \delta$, then $v \sim \delta^{k-1}$ and the result is the same as in case 2. For $v \sim \delta$, we have $u \sim \delta^{k-1}$ and the result is the same as in case 1.

Now suppose that $(\delta^k, b, c) = (\delta^i, b_1, c_1) \ast (\delta^j, b_2, c_2)$ where $b_1, b_2, c_1, c_2 \in \mathbb{Z}[i]$ and $i, j \in \mathbb{N}$. Since $(\delta^k, b, c)$ is primitive, $(\delta^i, b_1, c_1)$ and $(\delta^j, b_2, c_2)$ are primitive. By Lemma 2.7, $b_1, b_2, c_1, c_2$ are odd. Then $c = b_1b_2 + c_1c_2$ is even, a contradiction. Hence $(\delta^k, b, c)$ is irreducible.

The unique factorization of any primitive Pythagorean triple $(a, b, c)$ is reflected by the unique factorization of $a$, its first component. The following theorem shows how a primitive Pythagorean triple can be factored into a product of irreducible triples. We use the usual integer-exponent notation. For example, $A^2 = A \ast A$ for $A \in \text{PT}$.

**Proposition 2.16. (Unique factorization theorem)**

Let $A = (a, b, c) \in \text{PT}$ be primitive and $a = \delta^{s_0} p_1^{s_1} \cdots p_k^{s_k}$, where $p_i$ are distinct odd primes, $s_i$ are non-negative integers and $s_0 \neq 1, 2$. Then $A$ has the unique (up to order of factors and the multiplication of factors by units) factorization

$$A = P_0 \ast P_1^{s_1} \ast \ldots \ast P_k^{s_k}$$

where

$$P_0 \approx \begin{cases} (1, 0, 1) & \text{if } a \text{ is odd}, \\ (\delta^{s_0}, \pm(\delta^{2s_0-4} + 1), \delta^{2s_0-4} - 1) & \text{if } a \text{ is even} \end{cases}$$

and

$$P_i \approx (p_i, \pm \frac{p_i^2 - 1}{2}, \frac{p_i^2 + 1}{2})$$

for $i \geq 1$. The choice of $\pm$ depending on $(a, b, c)$.

**Proof.** There exist Gaussian integers $u, v, d$ where $d \mid 2$ and $d \mid u^2 \pm v^2$ such that

$$a = \frac{2uv}{d}, \quad b = \frac{u^2 - v^2}{d}, \quad \text{and } c = \frac{u^2 + v^2}{d}.$$
If $a$ is odd, then $d \sim 2$. We obtain

$$(a, b, c) \approx (uv, \frac{u^2 - v^2}{2}, \frac{u^2 + v^2}{2}) = (u, \frac{u^2 - 1}{2}, \frac{u^2 + 1}{2}) \ast (v, \frac{1 - v^2}{2}, \frac{1 + v^2}{2})$$

where the two triples on the right-hand side are elements in $PT$. Mathematical induction implies the factorization in this case.

In case that $a$ is even, $b$ and $c$ are odd by Lemma 2.7. The parity of $u$ and $v$ can be divided into 4 cases as follows:

Case 1: $u$ is even and $v$ is odd. Since $b = (u^2 - v^2)/d$ is odd, $d \sim 1$. Let $2u = \delta^k n$ where $n$ is an odd Gaussian integer and $k \in \mathbb{N}$. Then $(a, b, c) \approx (\delta^k, -((\delta^{2k-4} + 1), -((\delta^{2k-4} - 1))\ast (nv, (n^2 - v^2)/2, (n^2 + v^2)/2)$. Since $n$ and $v$ are odd, $(nv, (n^2 - v^2)/2, (n^2 + v^2)/2) \in PT$ is primitive. We then factor $(nv, (n^2 - v^2)/2, (n^2 + v^2)/2)$ as in the odd case.

Case 2: $u$ is odd and $v$ is even. This is similar to the above case.

Case 3: $u$ and $v$ are odd. Then $\delta^3$ does not divide $a$. This is a contradiction.

Case 4: $u$ and $v$ are even. Thus $u = \delta m$ and $v = \delta n$ for some $m, n \in \mathbb{Z}[i]$. Since $b = (u^2 - v^2)/d = (\delta^2 m^2 - \delta^2 n^2)/d$ is odd, we have $d \sim 2$ and $b \sim m^2 - n^2$. This means that $m$ and $n$ must have the different parity. Then $(a, b, c) \approx (2mn, m^2 - n^2, m^2 + n^2)$ which can be factored as in case 1 or case 2.

From the property that $(x, y, z) \ast (x, -y, z) = (x^2, 0, x^2)$ for all $(x, y, z) \in PT$, the choice $\pm$ of the term $P_i^{s_i}$ of $A$ cannot vary, otherwise $A$ would not be primitive. Since $a$ determines the first components of all factors of $A$, we assume that

$$A = P_0 \ast P_1^{s_1} \ast \ldots \ast P_k^{s_k} = Q_0 \ast Q_1^{s_1} \ast \ldots \ast Q_k^{s_k}$$

where for each $i$, $P_i$ and $Q_i$ are irreducible triples with identical first components. Now if $P = (x, y, z)$, we define $P' = (x, -y, z)$. If $P_j \approx Q_j$ for some $j$, it can be cancelled by multiplying $P'_j$ on both sides of the equation. Repeating this process until we have

$$P_{x_0} \ast P_{x_1} \ast \ldots \ast P_{x_m} = Q_{x_0} \ast Q_{x_1} \ast \ldots \ast Q_{x_m}$$

which is a factor of $A$ and $P_{x_i}$ does not associate $Q_{x_i}$. Propositions 2.10 and 2.15 and Lemma 2.12 show that $P_{x_i} \approx Q'_{x_i}$. Then, by multiplying the above equation by each of the $Q'_{x_i}$, we have

$$(P_{x_0} \ast P_{x_1} \ast \ldots \ast P_{x_m})^2 = (r^2, 0, r^2)$$

where the Gaussian integer $r$ is the product of the first components of $P_{x_i}$. It follows that $P_{x_0} \ast P_{x_1} \ast \ldots \ast P_{x_m} \approx (r, 0, r)$ which contradicts primitivity. This completes the proof.

Observe that $(l, 0, l) \ast (a, b, c) = (la, lb, lc)$. We will use the notation $l(a, b, c)$ for $(l, 0, l) \ast (a, b, c)$ in the next proposition which indicates how $(\delta^k, \pm(\delta^{2k-4} + 1), \delta^{2k-4} - 1)$ can be generated from $(\delta^3, \pm(\delta^2 + 1), \delta^2 - 1)$. 


Proposition 2.17. If \( k \geq 3 \) is an integer, then \( \delta^{2k-6}(\delta^k, \delta^{2k-4} + 1, \delta^{2k-4} - 1) \approx (\delta^3, \delta^2 + 1, \delta^2 - 1)^{k-2} \) and \( \delta^{2k-6}(\delta^k, -(\delta^{2k-4} + 1), \delta^{2k-4} - 1) \approx (\delta^3, -(\delta^2 + 1), \delta^2 - 1)^{k-2} \).

Proof. It is trivial when \( k = 3 \). For \( k > 3 \), \( \delta^2(\delta^k, \delta^{2k-4} + 1, \delta^{2k-4} - 1) \approx (\delta^3, \delta^2 + 1, \delta^2 - 1) \ast (\delta^{k-1}, \delta^{2k-6} + 1, \delta^{2k-6} - 1) \). Mathematical induction gives the desired result. When middle components have different signs the proof is similar. \( \square \)

Example 2.18. For the primitive triple \((96 + 72i, -24 + 151i, 24 + 137i)\) and \( 96 + 72i = \delta^6 \cdot 3 \cdot (1 + 2i)^2 \), Proposition 2.16 provides \((96 + 72i, -24 + 151i, 24 + 137i) = (\delta^6, \delta^8 + 1, \delta^8 - 1) \ast (3, 5i, 4i) \ast (1 + 2i, 2 - 2i, -1 + 2i)^2 \). By Proposition 2.17, \( \delta^6(96 + 72i, -24 + 151i, 24 + 137i) \) can be written as \((1, -i, 0) \ast (\delta^3, \delta^2 + 1, \delta^2 - 1)^4 \ast (3, 5i, 4i) \ast (1 + 2i, 2 - 2i, -1 + 2i)^2 \).

3 The Group of Primitive Pythagorean Triples Over Gaussian Integers

Definition 3.1. Let \((a, b, c), (d, e, f)\) be Pythagorean triples in \(\mathbb{Z}[i]\). We say that \((a, b, c)\) is equivalent to \((d, e, f)\) if there exists a nonzero element \(k \in \mathbb{Q}[i]\) such that \((a, b, c) = (kd, ke, kf)\). Denote the equivalence class of \((a, b, c)\) by \([a, b, c]\).

Since \(\mathbb{Z}[i]\) is a UFD, the set of all equivalence classes of Pythagorean triples may be considered as the set of all primitive Pythagorean triples. For this reason, let

\[
PPT = \{[a, b, c] \mid a, b, c \in \mathbb{Z}[i] \text{ with } a \neq 0; a^2 + b^2 = c^2\}
\]

be the set of all equivalence classes of Pythagorean triples in \(\mathbb{Z}[i]\) where first components are not zero. Define operation \(\ast\) as in (1). Note that the set of all Pythagorean triples, \(PT\), with the operation \(\ast\) is just a commutative monoid whereas the set of all equivalence classes, \(PPT\), under \(\ast\) is an abelian group.

Proposition 3.2. \((PPT, \ast)\) is an abelian group. The identity element in \(PPT\) is \([1, 0, 1]\), and the inverse of \([a, b, c]\) is \([a, -b, c]\).

Next we investigate a free abelian group, making use of the subgroup

\[
H := \{[1, 0, 1], [1, 0, -1], [1, i, 0], [1, -i, 0]\}
\]

of \(PPT\). Proposition 2.16, 2.17 and 3.2 give the following corollary.

Corollary 3.3. \((PPT/H, \ast)\) is a free abelian group which is generated by the set of \([a, b, c]H\) with \(a = \delta^3\) or \(a\) is an odd prime.
We establish an isomorphism between PPT and the multiplicative group of the quotient field $\mathbb{Q}[i]$ of $\mathbb{Z}[i]$.

**Proposition 3.4.** (PPT,*) is isomorphic to $(\mathbb{Q}[i]^\times, \cdot)$.

*Proof.* Define $\varphi : (\text{PPT},*) \to (\mathbb{Q}[i]^\times, \cdot)$ by $\varphi([a,b,c]) = (b+c)/a$. It is clear that $\varphi$ is well-defined.

Let $[a_1,b_1,c_1],[a_2,b_2,c_2] \in \text{PPT}$. Then $\varphi([a_1,b_1,c_1]*[a_2,b_2,c_2]) = \varphi([a_1a_2,b_1c_2 + b_2c_1,b_1b_2 + c_1c_2]) = (b_1b_2 + c_1c_2 + b_1c_2 + b_2c_1)/a_1a_2 = ((b_1 + c_1)/a_1) \cdot ((b_2 + c_2)/a_2)

= \varphi([a_1,b_1,c_1]) \cdot \varphi([a_2,b_2,c_2]).$

To show that $\varphi$ is injective, let $[a,b,c] \in \text{PPT}$ be such that $\varphi([a,b,c]) = 1$. Hence $(b+c)/a = 1$, i.e., $a = b + c$. Since $a^2 + b^2 = c^2$, we obtain $2b(b+c) = 0$. Then $b = 0$ or $b+c = 0$. But $b+c = a$ which is not 0, then $b = 0$ and $a = c$. Therefore, $[a,b,c] = [a,0] = [1,0,1]$ as desired.

Now let $u/v \in \mathbb{Q}[i]^\times$ where $u,v \in \mathbb{Z}[i] \setminus \{0\}$. Choose $a = 2uv, b = u^2 - v^2, c = u^2 + v^2 \in \mathbb{Z}[i]$. Then $\varphi([a,b,c]) = (b+c)/a = (u^2 + v^2 + u^2 - v^2)/2uv = u/v$. This implies that $\varphi$ is an isomorphism. 

In order to make PPT a field, we add $[0,1,1]$ into PPT and define operation addition $\oplus$ by using the isomorphism $\varphi$ between (PPT,*) and $(\mathbb{Q}[i]^\times, \cdot)$. The mapping $\phi : \text{PPT} \cup \{[0,1,1]\} \to \mathbb{Q}[i]$ given by

$$
\phi([a,b,c]) = \begin{cases} 
\varphi([a,b,c]) & \text{if } [a,b,c] \in \text{PPT}, \\
0 & \text{if } [a,b,c] = [0,1,1]
\end{cases}
$$

is both injective and surjective. Define operation $\oplus$ on $\text{PPT} \cup \{[0,1,1]\}$ by

$$
[a_1,b_1,c_1] \oplus [a_2,b_2,c_2] = \phi^{-1}(\phi([a_1,b_1,c_1]) + \phi([a_2,b_2,c_2])).
$$

It is not difficult to show the following proposition.

**Proposition 3.5.** (PPT$\cup\{[0,1,1]\}$, $\oplus$, *) is a field.

The set of Pythagorean triples with operation + defined by

$$(a_1,b_1,c_1) + (a_2,b_2,c_2) = (a_1a_2 - b_1b_2, a_1b_2 + b_1a_2, c_1c_2) \quad (4)$$

was also studied in term of its structure. In [6], P. Zanardo and U. Zannier described on a ring of integers $R$ such that $i \notin R$. In our case where $i \in \mathbb{Z}[i]$, let

$$
\mathbb{PPT} = \{[a,b,c] \mid a, b, c \in \mathbb{Z}[i] \text{ with } c \neq 0; a^2 + b^2 = c^2\}.
$$

With operation + in (4), $\mathbb{PPT}$ can be made into a group. The next proposition will show that (PPT,*) and (PPT,+) are isomorphic. Hence (PPT,+) is isomorphic to $(\mathbb{Q}[i]^\times, \cdot)$ as well.

**Proposition 3.6.** (PPT,*) is isomorphic to (PPT,+).
Proof. We need the fact that \([a, b, c] \in \text{PPT}\) if and only if \([c, bi, a] \in \text{PPT}\).

Define \(\lambda : (\text{PPT}, \ast) \rightarrow (\text{PPT}, +)\) by \(\lambda([a, b, c]) = [c, bi, a]\).

Let \([a_1, b_1, c_1], [a_2, b_2, c_2] \in \text{PPT}\). Then \(\lambda([a_1b_1c_1] \ast [a_2, b_2, c_2]) = \lambda([a_1a_2, b_1c_2 + b_2c_1, b_1b_2 + c_1c_2]) = [b_1b_2 + c_1c_2, (b_1c_2 + b_2c_1)i, a_1a_2] = [c_1c_2 - b_1ib_2i, c_1b_2i + c_2b_1i, a_1a_2]

\(\lambda([a_1, b_1, c_1]) + \lambda([a_2, b_2, c_2])\).

The rest of the proof comes from the above fact. \(\square\)

Let us remark that Definition 3.1, Proposition 3.2, 3.4 and 3.5 can be generalized to any ring of integers through similar proofs. Proposition 3.6 is also true for the ring of integers \(R\) in case that \(i \in R\).

References


Received: August, 2011