Quaternion

Hoon Kwon

March 13, 2010

Abstract

The concept of Quaternion is introduced here through the group and ring theory. The relationship between complex numbers (Gaussian Integers) and Quaternions can be verified by the basic properties and operations of Quaternions, which is represented by the matrix form of complex numbers. One can demonstrate the Fermats Two Square Theorem through Gaussian Integers while the Four Square Theorem with Quaternions is a result following this application. An efficient algorithm to compute the product of Quaternions will also be examined.

1 The Definition

Some simple group and ring theory will be introduced here for the understanding of Quaternion.

Definition 1.1. (Group). A non-empty set G is said to be a *group* if in G there is defined an operation $\times$ such that:

1. $a, b \in G$ implies that $a \times b \in G$. (i.e. G is closed under $\times$)
2. Given $a, b, c \in G$, then $a \times (b \times c) = (a \times b) \times c$
3. There exists $e \in G$ such that $a \times e = e \times a = a$ for all $a \in G$
4. For every $a \in G$ there exists an element $b \in G$ such that $a \times b = b \times a = e$. (We denote this element b as a^{-1})

These four conditions are called the *group axioms*, which are true for any given group. The operation $\times$ is usually called product. For simplicity we will omit it from now on. Hence $a \times b = ab$.

Definition 1.2. (Abelian Group). A group G is said to be *abelian* if $ab = ba$ for all $a, b \in G$.

Definition 1.3. (Ring). A *ring* is a set equipped with binary operations + and $\times$ and elements 0,1 such that R is an abelian group under +, and for all a,b,c $\in$ R we have

1. $1a = a1 = a$
2. $(ab)c = a(bc)$
3. $a(b+c) = ab + ac$

Definition 1.4. (division ring). A ring R with unit is said to be a *division ring* if for every $a \neq 0$ in R there is an element $b \in R$ (usually written as a^{-1}) such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$. That is there exists a multiplicative inverse for every nonzero element in R.

Definition 1.5. (Quaternions). Quaternions are a 4 turple non-communative ring over R^4 and in general writtin in the form $a = a_1 + a_2 i + a_3 j + a_4 k$, with the following operation defined.

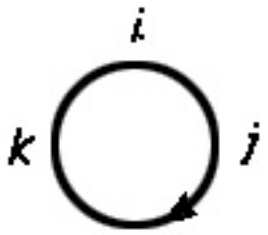

Figure 1: Going around the circle gives the product basis

let a, b be a Quaternions such $a = a_1 1 + a_2 i + a_3 j + a_4 k$, $b = b_1 1 + b_2 i + b_3 j + b_4 k$ and $i^2 = c, j^2 = d, ij = k, jk = i, ki = j$ and $ji = -k, kj = -i, ik = -j$

In the figure above, if one goes around the circle clockwise, the product of any two successive terms is the next one. By tracing around the circle counterclockwise, one will get negative products instead.

Addition $a + b = (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k$

Scalar Multiplication $sa = sa_1 + sa_2 i + sa_3 j + sa_4 k$

Quaternion Multiplication By following the distributive law, the product of two Quaternions can be written as

$$\begin{aligned} ab &= a_1 b_1 + a_1 b_2 i + a_1 b_3 j + a_1 b_4 k \\ &+ a_2 b_1 i + a_2 b_2 i^2 + a_2 b_3 ij + a_2 b_4 ik \\ &+ a_3 b_1 j + a_3 b_2 ji + a_3 b_3 j^2 + a_3 b_4 jk \\ &+ a_4 b_1 k + a_4 b_2 ki + a_4 b_3 kj + a_4 b_4 k^2 \end{aligned}$$

SAGE Example 1.6. *We demosntrate the Quaternion operations using SAGE.*

```
sage: N.<c,d,a1,a2,a3,a4,b1,b2,b3,b4,s> = QQ[]
sage: H.<i,j,k> = QuaternionAlgebra(c,d)
sage: a = a1 + a2 * i + a3 * j + a4 * k
sage: b = b1 + b2 * i + b3 * j + b4 * k
sage: a+b
a1 + b1 + (a2 + b2)*i + (a3 + b3)*j + (a4 + b4)*k
sage: s*a
a1*s + a2*s*i + a3*s*j + a4*s*k
```

```
sage: a*b
-x*y*a4*b4 + x*a2*b2 + y*a3*b3 + a1*b1
+( y*a4*b3 - y*a3*b4 +   a2*b1 + a1*b2)*i
+(-x*a4*b2 + x*a2*b4 +   a3*b1 + a1*b3)*j
+(   a4*b1 -   a3*b2 +   a2*b3 + a1*b4)*k
```

Definition 1.7. (Hamilton Quaternions). Hamilton Quaternions are Quaternions such that $i^2 = j^2 = k^2 = -1$.

Unless noted otherwise, Quaternions for now on will refer to Hamilton Quaternions.

SAGE Example 1.8. *We demosntrate the Hamilton Quaternion Multiplication using SAGE.*

```
sage: N.<a1,a2,a3,a4,b1,b2,b3,b4> = QQ[]
sage: H.<i,j,k> = QuaternionAlgebra(Frac(N),-1,-1)
   a1*b1 - a2*b2 - a3*b3 - a4*b4
+ (a2*b1 + a1*b2 - a4*b3 + a3*b4)*i
+ (a3*b1 + a4*b2 + a1*b3 - a2*b4)*j
+ (a4*b1 - a3*b2 + a2*b3 + a1*b4)*k
```

2 Two Square Theorem

In this section, we will show the Two Square Theorem, which is an example that some integers can be represented as a sum of two squares. This will be the basis for the later Four Square Theorem. Gaussian numbers and primes, Wilsons Theorem, and Lagranges lemma will be introduced for the Two Square Theorem proof.

Definition 2.1. (Gaussian integers). *Gaussian integer* is a complex number whose real and imaginary part are both integers. The Gaussian integers form a ring that is often denoted by $\mathbb{Z}[i]$. Gaussian integers are written

$$\mathbb{Z}[i] = \{a+bi | a,b \in \mathbb{Z}\}$$

The norm of a Gaussian integer is the natural number defined as

$$N(a+bi) = |a+bi| = a^2+b^2 = (a+bi)\overline{(a+bi)} = (a+bi)(a-bi)$$

Lemma 2.2. *The norm of the Gaussian integers is multiplicative*

Proof. Let z = a + bi, w = c + di

$$\begin{aligned} N(z\cdot w) &= |(a+bi)(c+di)| \\ &= |(ac-bd)+(ad+bc)i| \\ &= (ac-bd)^2+(ad+bc)^2 \\ &= a^2c^2+b^2d^2-2abcd+a^2d^2+b^2c^2+2abcd \\ &= a^2c^2+b^2d^2+a^2d^2+b^2c^2 \\ &= a^2(c^2+d^2)+b^2(c^2+d^2) \\ &= (a^2+b^2)(c^2+d^2) \\ &= |a+bi||c+di| \\ &= N(z)N(w) \end{aligned}$$

Definition 2.3. (Gaussian Prime). *Gaussian Prime* is a Gaussian integer that is not the product of Gaussian integers of smaller norm.

For example, we can show that $4+i$ is Gaussian prime.

$$\text{norm}(4+i) = 16+1 = 17, \text{which is a prime in } \mathbb{Z}$$

Hence, 4+i is not a product of Gaussian integers of smaller norm, since there is no such norm that divide 17.
Similarly, we can show that 2 is not Gaussian prime.

$$2 = (1+i)(1-i)$$

Both 1 - i and 1 + i have norm 2, which is smaller than norm(2) = 4

Lemma 2.4. *An ordinary prime $p \in \mathbb{N}$ is a Gaussian prime <=> p is not the sum of two squares.*

Proof.(<=) Suppose that we have an ordinary prime p that is not a Gaussian prime, so it can be factorized in $\mathbb{Z}[i]$:

$$p = (a+bi)\gamma,$$

where a + bi and γ are Gaussian integers where norm(p) $<$ norm(p^2). Taking the conjugates of both sides we get

$$p = (a-bi)\bar{\gamma},$$

since p is real, $p = \bar{p}$. Hence, by multiplying these two expressions

$$\begin{aligned} p^2 &= (a-bi)(a+bi)\gamma\bar{\gamma} \\ &= (a^2+b^2)|\gamma|^2 \end{aligned}$$

both $a^2+b^2, |\gamma|^2 > 1$. However the only such factorization of p^2 is $p \times p$, hence $p = a^2+b^2$.
(=>) Conversely, if an ordinary prime $p = a^2+b^2$ with a,b $\in \mathbb{Z}$ then p is not a Gaussian prime because it can be written as

$$p = (a-bi)(a+bi)$$

into factors of norm $a^2+b^2 = p < \text{norm}(p) = p^2$

Theorem 2.5. *(Wilson's theorem). If p is prime, then* $(p-1)! \equiv -1 (mod p)$.

Proof. If p = 2, then $(2-1)! = 1! = 1 \equiv -1 \, (mod p)$
Suppose p is a prime such that $p > 2$. If a $\in \{1, 2, ..., p-1\}$, then the equation

$$ax \equiv 1 \quad (mod p)$$

has a unique solution $a' \in \{1, 2, ..., p-1\}$. If $a = a'$, then $a^2 \equiv 1 \, (mod p)$. So, $a \in \{1, p-1\}$. We can thus pair off the elements of $\{2, 3, ..., p-2\}$, each with their inverse. Therefore,

$$\begin{aligned} 2 \cdot 3 \cdot \cdots \cdot (p-2) &\equiv 1 \, (mod p) \\ 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-2)(p-1) &\equiv (p-1) \, (mod p) \\ (p-1)! &\equiv -1 \, (mod p) \end{aligned}$$

Lemma 2.6. *(Lagrange's lemma). A prime* $p = 4n+1$ *divides* $m^2 + 1$ *for some* $m \in \mathbb{Z}$.

Proof. If we apply Wilson's theorem to the prime p = 4n+1 we get

$$\begin{aligned} -1 &\equiv 1 \times 2 \times \cdots \times 4n (mod p) \\ &\equiv (1 \times 2 \times \cdots \times 2n) \times ((2n+1) \times \cdots \times (4n-1) \times (4n)) (mod p) \\ &\equiv (1 \times 2 \times \cdots \times 2n) \times ((-2n) \times \cdots \times (-2) \times (-1)) (mod p) \quad \text{since } \; p - k \equiv (-k mod p) \\ &\equiv (1 \times 2 \times \cdots \times 2n)^2 (-1)^{2n} (mod p) \\ &\equiv (1 \times 2 \times \cdots \times 2n)^2 (mod p) \end{aligned}$$

Now we have laid out enough ground work to prove the Two Square Theorem

Theorem 2.7. *(Fermat's Two Square Theorem). An odd prime p is expressible as sum of two squares if and only if* $p \equiv 1 (mod 4)$.

Proof. Given p, let $m \in \mathbb{Z}$ be such that p divides $m^2 + 1$, as in the lemma 2.6. In $\mathbb{Z}[i]$, $m^2 + 1$ had the factorization

$$m^2 + 1 = (m - i)(m + i)$$

And, even though p divides $m^2 + 1$, p does not divide $m - i$ or $m + i$ because $\frac{m}{p} - \frac{i}{p}$ and $\frac{m}{p} + \frac{i}{p}$ are not Gaussian integers. Since $m^2 + 1$ is not a Gaussian prime (by definition 2.3), $p = a^2 + b^2$ as shown in Lemma 2.4

3 Complex Numbers and Quaternion Integers

In this section, the Quaternion is represented as complex numbers. Through the transformation of the Quaternion into a 2 by 2 matrix, we verify and observe the group properties of Quaternions.

Remark 3.1. Any given Quaternion can be written as two complex numbers.

Proof. Let $\mathbb{C}^2$ be a two-dimensional vector space over the complex numbers. Choose a basis consisting of two elements 1 and j. A vector in $\mathbb{C}^2$ can be written in terms of the basis elements 1 and j as

$$\begin{aligned}(a+bi)1+(c+di)j &= a+bi+cj+dij \\ &= a+bi+cj+dk\end{aligned}$$

Another way to represent a complex number is in the form of matrix. Let

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = aI + bi$$

Where, $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then we get the identity $i^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -1$.
Also norm$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a^2 + b^2 = det\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

Using these facts, we define a Quaternion as follow.

$$\begin{aligned}\text{Let } \alpha &= a+bi \\ \beta &= c+di \\ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} &= \text{ Quaternion}\end{aligned}$$

Then we observe the following facts.

$$\begin{aligned}\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} &= \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \\ &= a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + c\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} + d\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \\ &= a1+bi+cj+dk\end{aligned}$$

and we can verfiy the relationship

$$\begin{aligned}i^2 = j^2 = k^2 = -1 \\ ij = k = -ji \\ jk = i = -kj \\ ki = j = -ik\end{aligned}$$

Norm of Quaternion

$$\begin{aligned} \text{norm}\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} &= \alpha\overline{\alpha}+\beta\overline{\beta} \\ &= a^2+b^2+c^2+d^2 \\ &= \det\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \end{aligned}$$

Quaternion product

$$\begin{pmatrix} \alpha_1 & \beta_1 \\ -\overline{\beta_1} & \overline{\alpha_1} \end{pmatrix}\begin{pmatrix} \alpha_2 & \beta_2 \\ -\overline{\beta_2} & \overline{\alpha_2} \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2-\beta_1\overline{\beta_2} & \alpha_1\beta_2+\beta_1\overline{\alpha_2} \\ -\overline{\beta_1}\alpha_2-\overline{\alpha_1}\overline{\beta_2} & -\overline{\beta_1}\beta_2+\overline{\alpha_1}\alpha_2 \end{pmatrix}$$

We see that $\alpha_1\alpha_2-\beta_1 z\overline{\beta_2} = \overline{-\overline{\beta_1}\beta_2+\overline{\alpha_1}\alpha_2}$ and $\alpha_1\beta_2+\beta_1\overline{\alpha_2} = -(\overline{-\overline{\beta_1}\alpha_2-\overline{\alpha_1}\overline{\beta_2}})$

4 Four square theorem

In this section, we prove that any natural number can be expressed as the sum of four integer squares by using the Hurwitz Quaternion. This proof is similar to the Fermats Two Square Theorem (2.7) given in the previous section

Definition 4.1. (Hurwitz Quaternion). *Hurwitz Quaternion* is a Quaternion where the coefficients are either all integers or half-integers. The set of all Hurwitz Quaternion are denoted as

$$H = \{a+bi+cj+dk \in \mathbb{H} | a,b,c,d \in \mathbb{Z} \text{ or } a,b,c,d \in \mathbb{Z}+\frac{1}{2}\}$$

or

$$H = \{A\frac{1+i+j+k}{2}+Bi+Cj+Dk \in \mathbb{H} | A,B,C,D \in \mathbb{Z}\}$$

Remark 4.2. If p = 2n+1, then there are l,m $\in \mathbb{Z}$ such that p divides $1+l^2+m^2$

Proof. The squares x^2, y^2 of any two of the numbers $l = 0,1,2,...,n$ are incongurent mod p because

$$\begin{aligned} x^2 \equiv y^2 \ (mod p) &\Rightarrow x^2-y^2 \equiv 0 \ (mod p) \\ &\Rightarrow (x-y)(x+y) \equiv 0 \ (mod p) \\ &\Rightarrow x-y \equiv 0 \ (mod p) \text{ to } x+y \equiv 0 \ (mod p) \end{aligned}$$

and x+y$\not\equiv$ 0 (mod p) since $0 < x+y < p$. Thus the n+1 numbers $l = 0,1,2,...,n$ gives n+1 incongruent values of $l^2(mod p)$
Similarly, the numbers $m = 0,1,2,...,n$ also gives n+1 incongruent values of $m^2(mod p)$, hence $-m^2$ which is $-1-m^2$

However, only 2n+1 incongruent values exist for mod p = 2n +1. Therefore, for some l and m we have

$$l^2 \equiv -1 - m^2 \text{ (mod p)}$$

That is, $p|1+l^2+m^2$.

Theorem 4.3. *(Four square theorem). Every natural number is the sum of four square.*

Proof. If $q = a1 + bi + cj + dk$ then norm(q) is

$$\det \begin{pmatrix} a+di & b+ci \\ -b+ci & a-di \end{pmatrix} = a^2+b^2+c^2+d^2$$

Since $det(q_1)det(q_2) = det(q_1q_2)$, we can rewrite the *complex two square identity* as a *real four square identity*, which becomes

$$\begin{aligned}(a_1^2+b_1^2+c_1^2+d_1^2)(a_2^2+b_2^2+c_2^2+d_2^2) &= (a_1a_2-b_1b_2-c_1c_2-d_1d_2)^2 \\ &+ (a_1b_2+b_1a_2+c_1d_2-d_1c_2)^2 \\ &+ (a_1c_2-b_1d_2+c_1a_2+d_1b_2)^2 \\ &+ (a_1d_2+b_1c_2-c_1b_2+d_1a_2)^2\end{aligned}$$

Hence, we have,

$$\begin{aligned}(a_1^2+b_1^2+c_1^2+d_1^2) &= ((a_1a_2-b_1b_2-c_1c_2-d_1d_2)^2 \\ &+ (a_1b_2+b_1a_2+c_1d_2-d_1c_2)^2 \\ &+ (a_1c_2-b_1d_2+c_1a_2+d_1b_2)^2 \\ &+ (a_1d_2+b_1c_2-c_1b_2+d_1a_2)^2) \\ &\times \frac{1}{a_2^2+b_2^2+c_2^2+d_2^2}\end{aligned}$$

Now we consider the following two cases.
if p is an ordinary prime but not a Hurwitz prime, then

$$p = a^2+b^2+c^2+d^2 \text{ where } 2a, 2b, 2c, 2d \in \mathbb{Z}$$

Proof. Suppose p has a nontrivial Hurwitz integer factorization

$$p = (a+bi+cj+dk)\gamma$$

Then, taking the conjugates of both sides, we get

$$p = \overline{\gamma}(a-bi-cj-dk), \text{ since } \overline{p} = p$$

Multiplying the two expressions for p gives

$$\begin{aligned}p^2 &= (a+bi+cj+dk)\gamma\overline{\gamma}(a-bi-cj-dk) \\ &= (a+bi+cj+dk)(a-bi-cj-dk)\gamma\overline{\gamma} \text{ since } \gamma\overline{\gamma} \text{ is real} \\ &= (a^2+b^2+c^2+d^2)|\gamma|^2,\end{aligned}$$

where both $a^2+b^2+c^2+d^2$, $|\gamma|^2 > 1$. But the only positive integer factorization of p^2 is pp, hence $a^2+b^2+c^2+d^2$.
Finally, since a,b,c,d, are the coefficients of a Hurwitz integer, they could be half integers, which in case $2a, 2b, 2c, 2d \in \mathbb{Z}$
The last case to consider is for any odd prime p, which by Remark 4.2 above, we have shown $p|1+l^2+m^2$.
We factorize $1+l^2+m^2$ into the product of Hurwitz integers

$$(1-li-mj)(1+li+mj)$$

If p is a Hurwitz prime, then p divides $(1-li-mj)$ or $(1+li+mj)$. However,

$$\frac{1}{p}-\frac{li}{p}-\frac{mj}{p}, \frac{1}{p}+\frac{li}{p}+\frac{mj}{p}$$

are both not a Hurwitz integer. Hence our arbitary odd prime p is not a Hurwithz prime, and therefore by the previous argument

$$p = A^2+B^2+C^2+D^2 \text{ with } A,B,C,D \in \mathbb{Z}$$

is shown for the Four Square Theorem.

5 Fast Quaternion Products

In general to compute the product of two Quaternion, namely $X = x_1+x_2i+x_3j+x_4k$ and $Y = y_1+y_2i+y_3j+y_4k$ their product is:

$$\begin{aligned} XY &= x1*y1-x2*y2-x3*y3-x4*y4 \\ &+ (x2*y1+x1*y2-x4*y3+x3*y4)*i \\ &+ (x3*y1+x4*y2+x1*y3-x2*y4)*j \\ &+ (x4*y1-x3*y2+x2*y3+x1*y4)*k \end{aligned}$$

This would normally require 16 multiplications. To reduce the complexity of Quaternion product computation, reducing the number of multiplications is crucial. Here we show an algorithm that needs eight multiplications to correctly compute the product of the Quaternions.
Let $Z = XY = z_1+z_2i+z_3j+z_4k$ where,

$$\begin{aligned} z_1 &= x1*y1-x2*y2-x3*y3-x4*y4, \\ z_2 &= x2*y1+x1*y2-x4*y3+x3*y4, \\ z_3 &= x3*y1+x4*y2+x1*y3-x2*y4, \\ z_4 &= x4*y1-x3*y2+x2*y3+x1*y4 \end{aligned}$$

Define the following. Let

$$\begin{aligned} I &= x_1y_1 \\ II &= x_4y_3 \\ III &= x_2y_4 \\ IV &= x_3y_2 \\ V &= (x_1+x_2+x_3+x_4)(y_1+y_2+y_3+y_4) \\ VI &= (x_1+x_2-x_3-x_4)(y_1+y_2-y_3-y_4) \\ VII &= (x_1-x_2+x_3-x_4)(y_1-y_2+y_3-y_4) \\ VIII &= (x_1-x_2-x_3+x_4)(y_1-y_2-y_3+y_4) \end{aligned}$$

Then the each z_i equals the following

$$\begin{aligned} z_1 &= 2I - \frac{V+VI+VII+VIII}{4} \\ z_2 &= -2II + \frac{V+VI-VII-VIII}{4} \\ z_3 &= -2III + \frac{V-VI+VII-VIII}{4} \\ z_4 &= -2IV + \frac{V-VI-VII+VIII}{4} \end{aligned}$$

This way we will only have to compute 8 multiplications at most.

SAGE Example 5.1. *We verify the equailty in SAGE.*

```
sage: N.<a1, a2, a3, a4, b1, b2, b3, b4> = QQ[]
sage: H.<ii,jj,kk> = QuaternionAlgebra(Frac(N), -1, -1)
sage: a = a1 + a2*i + a3*j + a4*k
sage: b = b1 + b2*i + b3*j + b4*k
sage: c = a*b; c
    a1*b1 - a2*b2 - a3*b3 - a4*b4
 + (a2*b1 + a1*b2 - a4*b3 + a3*b4)*i
 + (a3*b1 + a4*b2 + a1*b3 - a2*b4)*j
 + (a4*b1 - a3*b2 + a2*b3 + a1*b4)*k
sage: I = a1*b1
sage: II = a4*b3
sage: III= a2*b4
sage: IV = a3*b2
sage: V = (a1+a2+a3+a4)*(b1+b2+b3+b4)
```

```
sage: VI = (a1+a2-a3-a4)*(b1+b2-b3-b4)
sage: VII = (a1-a2+a3-a4)*(b1-b2+b3-b4)
sage: VIII= (a1-a2-a3+a4)*(b1-b2-b3+b4)
sage: f1 = 2*I - (V + VI + VII + VIII)/4
sage: f2 = -2*II + (V + VI - VII - VIII)/4
sage: f3 = -2*III + (V - VI + VII - VIII)/4
sage: f4 = -2*IV + (V - VI - VII + VIII)/4
sage: q3 = f1 + f2*i + f3*j + f4*k; q3
   a1*b1 - a2*b2 - a3*b3 - a4*b4
+ (a2*b1 + a1*b2 - a4*b3 + a3*b4)*i
+ (a3*b1 + a4*b2 + a1*b3 - a2*b4)*j
+ (a4*b1 - a3*b2 + a2*b3 + a1*b4)*k
sage: c == q3
True
```

SAGE Example 5.2. *The following is the SAGE implementation of the normal(lame) and the fast algorithm*

```
sage: def slow_mult((x1, x2, x3, x4), (y1, y2, y3, y4)):
...       a1 = x1*y1; a2 = x2*y2; a3 = x3*y3; a4 = x4*y4
...       b1 = x1*y2; b2 = x2*y1; b3 = x3*y4; b4 = x4*y3
...       c1 = x1*y3; c2 = x2*y4; c3 = x3*y1; c4 = x4*y2
...       d1 = x1*y4; d2 = x2*y3; d3 = x3*y2; d4 = x4*y1
...       A = a1 - a2 - a3 - a4
...       B = b1 + b2 + b3 - b4
...       C = c1 - c2 + c3 + c4
...       D = d1 + d2 - d3 + d4
...       return (A,B,C,D)
sage: slow_mult((1,2,3,4),(1,2,3,4))
(-28, 4, 6, 8)
sage: def fast_mult((a1, a2, a3, a4), (b1, b2, b3, b4)):
...       I = a1*b1; II = a4*b3; III= a2*b4; IV = a3*b2
...       V = (a1+a2+a3+a4)*(b1+b2+b3+b4)
...       VI = (a1+a2-a3-a4)*(b1+b2-b3-b4)
...       VII = (a1-a2+a3-a4)*(b1-b2+b3-b4)
...       VIII= (a1-a2-a3+a4)*(b1-b2-b3+b4)
...
...       f1 = 2*I - (V + VI + VII + VIII)/4
...       f2 = -2*II + (V + VI - VII - VIII)/4
...       f3 = -2*III + (V - VI + VII - VIII)/4
...       f4 = -2*IV + (V - VI - VII + VIII)/4
...
...       return (f1, f2, f3, f4)
```

```
sage: fast_mult((1,2,3,4), (1,2,3,4))
(-28, 4, 6, 8)
sage: a = int(random()*2^10); b = int(random()*2^10);
sage: c = int(random()*2^10); d = int(random()*2^10);
sage: e = int(random()*2^10); f = int(random()*2^10);
sage: g = int(random()*2^10); h = int(random()*2^10);
sage: timeit('slow_mult((a,b,c,d), (e, f, g, h))')
625 loops, best of 3: 1.91 s per loop
sage: timeit('fast_mult((a,b,c,d), (e,f,g,h))')
625 loops, best of 3: 24.6 s per loop
sage: a = int(random()*2^768); b = int(random()*2^768);
sage: c = int(random()*2^768); d = int(random()*2^768);
sage: e = int(random()*2^768); f = int(random()*2^768);
sage: g = int(random()*2^768); h = int(random()*2^768);
sage: timeit('slow_mult((a,b,c,d), (e, f, g, h))')
625 loops, best of 3: 151 s per loop
sage: timeit('fast_mult((a,b,c,d), (e,f,g,h))')
625 loops, best of 3: 118 s per loop
```

One can see that when the coefficients are small, the computation does not make any significant improvement. However, if we use 768bit numbers, then a reduced number of multiplications in this algorithm provide greater efficiency for the Quaternion multiplication process.

References

[1] On the complexity of quaternion multiplication, 1975

[2] Abstract Algebra. New York: Macmillan, 1986.

[3] Elementary Number Theory: Primes, Congruences, and Secrets. Undergraduate texts in mathematics. New York: Springer, 2009.

[4] Elements of Number Theory. Undergraduate texts in mathematics. New York: Springer, 2003.

[5] Gaussian Elimination is not Optimal, Numer. Math. 13, p. 354-356, 1969

[6] Introduction to Abstract Algebra. Glasgow: Blackie Academic & Professional, an imprint of Chapman & Hall, 1995.