QUARTERNIONS AND THE FOUR SQUARE THEOREM

JIA HONG RAY NG

Abstract. The Four Square Theorem was proved by Lagrange in 1770: *every positive integer is the sum of at most four squares of positive integers, i.e.* $n = A^2 + B^2 + C^2 + D^2, A, B, C, D \in \mathbb{Z}$ An interesting proof is presented here based on Hurwitz integers, a subset of quarternions which act like integers in four dimensions and have the prime divisor property. It is analogous to Fermat's Two Square Theorem, which says that *positive primes of the form 4k+1 can be written as the sum of the squares of two positive integers.* Representing integers as the sum of squares can be considered a special case of Waring's problem: *for every k is there a number g (k) such that every integer is representable by at most g (k) k^{th} powers?*

Contents

1. Quarternions and Hurwitz Integers 1
2. Four Square Theorem 4
3. Discussion 6
References 6

1. Quarternions and Hurwitz Integers

Definition 1.1. For each pair $\alpha, \beta \in \mathbb{C}$, a quarternion is a four dimensional number represented by the matrix $q = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}$.

The set of quarternions is called $\mathbb{H}$, after its discoverer Hamiltion (1843). If $\alpha = a + di$ and $\beta = b + ci$, where $a, b, c, d \in \mathbb{R}$, then each quarternion is a linear combination of the quarternion units **1,i,j,k**.

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}$$
$$= \begin{pmatrix} a+di & b+ci \\ -b+ci & a-di \end{pmatrix}$$
$$= \mathrm{a}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \mathrm{b}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + \mathrm{c}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} + \mathrm{d}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$
$$= \mathrm{a}\mathbf{1} + \mathrm{b}\mathbf{i} + \mathrm{c}\mathbf{j} + \mathrm{d}\mathbf{k}$$

Definition 1.2. The norm of a quarternion, $\|q\|$ is defined to be the square root of its determinant, hence $\|q\|^2$ is

$$det\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix} = \alpha\overline{\alpha}+\beta\overline{\beta} = |\alpha|^2+|\beta|^2$$

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

The quarternions **1, i, j, k** have norm 1 and satisfy the following relations:

$$\mathbf{i}^2=\mathbf{j}^2=\mathbf{k}^2=-\mathbf{1},$$
$$\mathbf{ij}=\mathbf{k}=-\mathbf{ji},$$
$$\mathbf{jk}=\mathbf{i}=-\mathbf{kj},$$
$$\mathbf{ki}=\mathbf{j}=-\mathbf{ik}$$

Non-zero quarternions form a group under multiplication, but the product of quarternions is generally non-commutative: $q_1q_2 \neq q_2q_1$. Quarternions also form an abelian group under addition, and obey the left and right distributive laws: $q_1(q_2+q_3) = q_1q_2+q_1q_3, (q_2+q_3) = q_2q_1+q_3q_1$.

Due to the multiplicative property of the determinants, $det(q_1)\,det(q_2) = det(q_1q_2)$, the norm also has a multiplicative property, i.e.

$$norm(q_1)\,norm(q_2) = norm(q_1q_2).$$

It is interesting to note that $n = 1, 2, 4, 8$ are the only n for which $\mathbb{R}^n$ has a multiplication that distributes over vector addition, and a multiplicative norm. They correspond to $\mathbb{R}, \mathbb{C}, \mathbb{H}$ and $\mathbb{O}$ (the octonions, $n = 8$) respectively.

Theorem 1.3. *Four Square Identity: If two numbers can each be written as the sum of four squares, then so can their product.*

Proof. Let $x_1 = a_1^2+b_1^2+c_1^2+d_1^2 = \|a_1\mathbf{1}+b_1\mathbf{i}+c_1\mathbf{j}+d_1\mathbf{k}\|^2 = \|q_1\|^2$ and $x_2 = a_2^2+b_2^2+c_2^2+d_2^2 = \|a_2\mathbf{1}+b_2\mathbf{i}+c_2\mathbf{j}+d_2\mathbf{k}\|^2 = \|q_2\|^2$
Then by the multiplicative property of norms,
$x_1x_2 = \|q_1\|^2\|q_2\|^2 = \|q_1q_2\|^2$
Therefore, $x_1x_2 = a^2+b^2+c^2+d^2$, where $\|q_1q_2\|^2 = a^2+b^2+c^2+d^2$ □

Definition 1.4. The conjugate of any quarternion $q = a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$ is $\overline{q} = a-b\mathbf{i}-c\mathbf{j}-d\mathbf{k}$. Conjugation has the following easily-proved properties:

$$q\overline{q} = |q|^2,$$
$$\overline{q_1+q_2} = \overline{q_1}+\overline{q_2},$$
$$\overline{q_1-q_2} = \overline{q_1}-\overline{q_2},$$
$$\overline{q_1q_2} = \overline{q_2}\,\overline{q_1}$$

(due to non-commutative quarternion multiplication).

Definition 1.5. The Hurwitz integers are quarternions that make up the set of all the integer combinations of $\frac{\mathbf{1}+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2}, \mathbf{i}, \mathbf{j}, \mathbf{k}$, denoted by $\mathbb{Z}[\mathbf{h}, \mathbf{i}, \mathbf{j}, \mathbf{k}]$, where $\mathbf{h} = \frac{\mathbf{1}+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2}$. It contains the set $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}] = \{a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} : a, b, c, d \in \mathbb{Z}\}$. There are 24 units (that form a non-abelian group): the 8 units $\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}+\pm\mathbf{k}$ of $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$, and the 16 mid-points $\pm\frac{1}{2} \pm \frac{\mathbf{i}}{2} \pm \frac{\mathbf{j}}{2} \pm \frac{\mathbf{k}}{2}$. The Hurwitz integers are closed under addition and multiplication and the square of the norm is always an ordinary integer.

They also obey the division property, which says:
If $\alpha, \beta \neq 0$ are in $\mathbb{Z}[\boldsymbol{h}, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}]$, then there is a quotient μ and a remainder ρ such that $\alpha = \mu\beta + \rho$ with $|\rho| < |\beta|$.

Since multiplication of quarternions is not commutative, there are two kinds of divisors for each Hurwitz integer –left and right divisors. Given Hurwitz integers α, δ, γ, call δ a right divisor of α if $\alpha = \gamma\delta$ for some γ, and similarly for left divisors.

Definition 1.6. A Hurwitz integer p is prime if it is divisible only by the units of $\mathbb{Z}[\mathbf{h}, \mathbf{i}, \mathbf{j}, \mathbf{k}]$ and units times p.
The multiplicative property of the norm implies that: *if a Hurwitz integer α divides another Hurwitz integer γ, then norm(α) divides norm(γ).*

$$\gamma = \alpha\beta \text{ for some } \beta \in \mathbb{Z}[\mathbf{h}, \mathbf{i}, \mathbf{j}, \mathbf{k}] \Rightarrow \text{norm}(\gamma) = \text{norm}(\alpha)\,\text{norm}(\beta).$$

For example, consider $\frac{5+5\mathbf{i}+3\mathbf{j}+3\mathbf{k}}{2} = 5\frac{\mathbf{1}+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2} - \mathbf{j} - \mathbf{k}$. Its norm is

$$\frac{5^2 + 5^2 + 3^2 + 3^2}{4} = \frac{68}{4} = 17.$$

Since 17 is an ordinary prime, $\frac{5+5\mathbf{i}+3\mathbf{j}+3\mathbf{k}}{2}$ is not the product of Hurwitz integers of smaller norm. Therefore, it is a Hurwitz prime.

Definition 1.7. The Euclidean Algorithm is a method to find the greatest common divisor (gcd) of any two natural numbers, and can be applied to Hurwitz integers as well. The steps are as follow:
Suppose that $|\alpha| < |\beta|$, let $\alpha_1 = \alpha$ and $\beta_1 = \beta$.
Then for each pair (α_i, β_i), produce the next pair by the rule,

$$\alpha_{i+1} = \beta_i, \beta_{i+1} = \text{ remainder when } \alpha_i \text{ is divided by } \beta_i.$$

(The remainder β_{i+1} is less than the divisor β_i by the division property described in Definition 1.5.)
Now if α and β have a common right divisor δ, then

$$\alpha = \gamma\delta,\ \beta = \varepsilon\delta \text{ for some } \gamma, \varepsilon,$$

Therefore $\rho = \alpha - \mu\beta = \gamma\delta - \mu\varepsilon\delta = (\gamma - \mu\varepsilon)\,\delta$.
This means that a common right divisor of α and β is also a right divisor of the remainder ρ when α is divided on the right by β. Therefore

$$\text{right gcd}(\alpha_1, \beta_1) = \text{right gcd}(\alpha_2, \beta_2) = \ldots$$

The algorithm stops when α_k divides α_k, such that $g = \text{right gcd}(\alpha, \beta) = \text{right gcd}(\alpha_k, \beta_k) = \beta_k$.

Theorem 1.8. *Linear Representation of Greatest Common Divisor: If g is the greatest common divisor of α and β, then $g = \gcd(\alpha, \beta) = \mu\alpha + \nu\beta$ for some integers μ and ν.*
The theorem can be easily proved by induction on the number pairs obtained from the Euclidean algorithm, starting with

$$\alpha_1 = 1 \times \alpha + 0 \times \beta, \quad \beta_1 = 0 \times \alpha + 1 \times \beta.$$

Theorem 1.9. *Prime Divisor Property of Hurwitz Integers: if p is a real Hurwitz prime and divides a Hurwitz integer product $\alpha\beta$, then p divides α or p divides β.*

Proof. Assume that the prime p divides $\alpha\beta$ but does not divide α. Then according to Theorem 1.8,

$$1 = \text{right gcd}\,(p, \alpha) = \mu p + \nu\alpha.$$

Multiplying on the right by β for both sides,

$$\beta = \mu p\beta + \nu\alpha\beta.$$

Note that p is both a right and left divisor of whatever number it divides, since reals commute with quarternions. Therefore p divides both $\mu p\beta$, and $\nu\alpha$ (by assumption). Consequently, p divides β, as required by the statement. □

2. Four Square Theorem

Now, we can use the above properties of quarternions to prove the Four Square Theorem, which says that *every natural number is the sum of four squares.* In fact, the Four Square Identity (Theorem 1.3) implies that if every prime is the sum of four squares, then all the other natural numbers except 1, which are products of primes, can satisfy the Four Square Theorem. Clearly, $1 = 0^2 + 0^2 + 0^2 + 1^2$ and $2 = 0^2 + 0^2 + 1^2 + 1^2$, therefore we can immediately simplify the problem to that of representing every odd prime p as the sum of four integer squares. The following proof is due to Hurwitz himself, and differs from Lagrange's own proof, which argues that the least integer m satisfying the equation $mp = A^2 + B^2 + C^2 + D^2$ is 1.

Theorem 2.1. *(Conditional Four Square Theorem): any ordinary prime p that is not a Hurwitz prime is a sum of four integer squares.*

Proof. Suppose p has a nontrivial Hurwitz integer factorization

$$p = (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})\,\gamma$$

Taking conjugates on both sides,

$$p = \overline{p} = \overline{\gamma}\,(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k})$$

Multiplying both expressions,

$$\begin{aligned} p^2 &= (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})\,\gamma\overline{\gamma}\,(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) \\ &= (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})\,(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k})\,\gamma\overline{\gamma} \\ &= \left(a^2 + b^2 + c^2 + d^2\right)|\gamma|^2 \end{aligned}$$

where both $a^2 + b^2 + c^2 + d^2$ and $|\gamma|^2$ are integers greater than 1. However, by unique prime factorization, the only positve integer factorization is pp, therefore $p = a^2 + b^2 + c^2 + d^2 = (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})\,(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k})$. If the Hurwitz integer $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ is also in the set $\mathbb{Z}\,[\mathbf{i}, \mathbf{j}, \mathbf{k}]$, then p is the sum of four integer squares.

But suppose $\psi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ has half-integer co-ordinates, the factors of p^2 can be re-expressed to achieve integer values for the co-efficients of $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ in ψ. Consider the integer $\omega = \frac{\pm\mathbf{1}\pm\mathbf{i}\pm\mathbf{j}\pm\mathbf{k}}{2}$, which has norm 1, thus $\omega\overline{\omega} = 1$. By choosing appropriate signs in ω, ψ can be written as $\psi = \omega + a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}$, where a', b', c', d' are even integers. Therefore,

$$\begin{aligned} p &= (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})\,(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) \\ &= (\omega + a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k})\,(\omega + a' - b'\mathbf{i} - c'\mathbf{j} - d'\mathbf{k}) \\ &= (\omega + a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k})\,\overline{\omega} \times \omega\,(\omega + a' - b'\mathbf{i} - c'\mathbf{j} - d'\mathbf{k}) \end{aligned}$$

With respect to the first factor, the product of $\overline{\omega}$ and ω plus the even terms gives 1 plus integer terms, hence the first factor is $A+B\mathbf{i}+C\mathbf{j}+D\mathbf{k}$ for some $A, B, C, D \in \mathbb{Z}$. The second factor is its conjugate, thus

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

□

The following lemma is useful for showing that every odd prime is not a Hurwitz prime, which combined with Theorem 2.1, implies that every odd prime can be expressed as the sum of four squares.

Lemma 2.2. *If an odd prime $p = 2n + 1$, 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 0,1,2,...,n are incongruent mod p because

$$\begin{gathered} x^2 \equiv y^2 \pmod{p} \Rightarrow x^2 - y^2 \equiv 0 \pmod{p} \\ (x-y)(x+y) \equiv 0 \pmod{p} \\ x \equiv y \text{ or } x+y \equiv 0 \pmod{p} \end{gathered}$$

$x + y \not\equiv 0 \pmod{p}$ since $0<x + y<p$. Therefore the $n + 1$ different numbers $l = 0, 1, 2, \ldots, n$ give $n + 1$ incongruent values of $l^2 \mod p$. Similarly, there are $n + 1$ incongruent values of $m^2 \mod p$ and hence of $-1 - m^2 \mod p$, where $m = 0, 1, 2, \ldots, n$ But there only exist $2n + 1$ incongruent values, $\mod p = 2n + 1$. Therefore, by the pigeon-hole principle, for some l and m,

$$\begin{gathered} l^2 \equiv -1 - m^2 \pmod{p} \\ 1 + l^2 + m^2 \equiv 0 \pmod{p} \end{gathered}$$

□

Theorem 2.3. *Four Square Theorem: Every natural number is the sum of four squares.*

Proof. Let p be an odd prime. Then we can find l and m such that p divides $1 + l^2 + m^2$ (by Lemma 2.2)
Factorizing it,

$$1 + l^2 + m^2 = (1 + l\mathbf{i} + m\mathbf{j})(1 - l\mathbf{i} - m\mathbf{j})$$

If p were a Hurwitz prime, then, according to the prime divisor property (Theorem 1.9), p divides either $1+l\mathbf{i}+m\mathbf{j}$ or $1-l\mathbf{i}-m\mathbf{j}$ But neither case is possible, since neither

$$\frac{1}{p} + \frac{l\mathbf{i}}{p} + \frac{m\mathbf{j}}{p} \text{ nor } \frac{1}{p} - \frac{l\mathbf{i}}{p} - \frac{m\mathbf{j}}{p}$$

is a Hurwitz integer. Hence the arbitrary odd prime p is not a Hurwitz prime, and by Theorem 2.1,

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

By the four square identity (Theorem 1.3), every natural number is the sum of four squares. □

3. Discussion

The Four Square Theorem was first conjectured in Bachet's 1621 edition of Diophantus and the first proof was given by Lagrange in 1770. Fermat claimed to have come up with a proof, but did not publish it. In fact, there is a similar theorem called Fermat's Two Square Theorem, that is a corollary of the Four Squares Theorem.

Theorem 3.1. *Two Square Theorem: if $p = 4n + 1$ is prime, then $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.*

A proof exists that uses the unique prime factorization of Gaussian integers $\mathbb{Z} = \{a + bi : a, b \in \mathbb{Z}\}$ and Lagrange's lemma, *a prime $= 4n + 1$ divides $m^2 + 1$ for some $m \in \mathbb{Z}$.*

It has also been shown that only the numbers for which primes of the form 4k-1 do not appear to an odd power in their canonical decomposition can be represented as the sum of two squares. Thus, not all natural numbers can be expressed as the sum of two squares.

It is a similar situation for the sum of three squares, as it has been proved that numbers of the form $4^n (8k + 7)$ cannot be expressed as the sum of three squares. This proof is more involved than those for sums of two or four squares and is due to the fact that a three square identity does not exist, i.e. the product of two sums of three squares is not always a sum of three squares.

Waring generalized the question about the expression of numbers as the sum of squares to higher powers.

Theorem 3.2. *Waring's problem: There is a number $g(k)$ for every positive integer k such that every integer can be written as at most $g(k)$ k^{th} powers.*

For example, g(2) is 4, g(3) is 9, g(4) is 19, g(5) is 37 and g(6) is 73. Euler conjectured that $g(k) \geqslant 2^k + \lfloor \left(\frac{3}{2}\right)^k \rfloor$ and Dickson, Pillai and Niven later conjectured that the equality holds provided $2^k \left\{ \left(\frac{3}{2}\right)^k \right\} + \lfloor \left(\frac{3}{2}\right)^k \rfloor \geqslant 2^k$, where $\{x\}$ denotes the fractional part of x. This equality has been proven to be correct for $6 \leq n \leq 471600000$, but it is uncertain if it holds for all values of n.

References

[1] J Stillwell. Elements of Number Theory. Springer-Verlag New York Inc. 2003.
[2] P Erdos, J Suranyi. Topics in the Theory of Numbers (2nd Ed). Springer-Verlag New York Inc. 2003.
[3] I Niven, H S Zuckerman. Introduction to the Theory of Numbers (2nd Ed). John Wiley Sons, Inc. 1966.
[4] Weisstein, Eric W. "Waring's Problem." From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/WaringsProblem.html