THE REPRESENTATION OF A NUMBER BY TWO OR FOUR SQUARES

GEORGE ROBERT WOODBURY

Abstract. In this paper I discuss the classical theorems of Fermat and Lagrange on the representability of numbers by two or four squares. A common theme is the use of number systems beyond Z (Gaussian integers and Hurwitz integers respectively) to solve problems that are stated within the integers.

Contents

1. Introduction

Fermat's two square theorem

The two square theorem, as it is known today, was stated without proof by Fermat in 1640, though he claimed to have a proof by descent: assuming a prime p that is of the form 4n + 1 but not a sum of two squares, one could show that there is a smaller prime with the same property. The first known proof of the theorem was in fact by descent, and published by Euler (1755). It cost him several years of effort.

In order to prove Fermat's two square theorem, I shall rely on what is known as the Gaussian integers. We apply the theory of Z[**i**] (the set of Gaussian integers) to a prime $p = 4n + 1$ with the help of an $m \in Z$ such that p divides $m^2 + 1$ by a result of Lagrange (1773) that follows from Wilson's theorem. This proof assumes basic knowledge of congruence and complex numbers.

Lagrange's four square theorem

The next theorem provided in this paper, the four square theorem, states that every natural number is the sum of four integer squares. The theorem was first proved in 1770 by Joseph Louis Lagrange, and because of his contribution the theorem is known today as Lagrange's four square theorem.

To solve Lagrange's four square theorem, I shall prove that every prime is the sum of four squares. This fact is sufficient due to the factorization of every number into primes, and the four square identity of Euler which states that the product of

two numbers that are the sum of four squares yields a number that is itself the sum of four squares. This proof also assumes basic knowledge of complex numbers, but also of linear algebra.

2. Fermat's Two Square Theorem

Definition 2.1. The *Gaussian integers* are the set

$$\mathrm{Z}[\mathbf{i}] = \{a + b\mathbf{i} \in \mathrm{C} : a, b \in \mathrm{Z}\}.$$

Note that the set of Gaussian integers is closed under addition, subtraction and multiplication, therefore we can think of this as a generalized number system, hence the name Gaussian integers.

Theorem 2.2 (Wilson's theorem)**.** *If p is prime then*

$$(p-1)! \equiv -1 \bmod p.$$

Proof. In this congruence the factors $1, 2, 3, \ldots, p-1$ all have inverses mod p, hence each is cancelled by its own inverse except the factors that are the inverse of them- selves.

Such self-inverse factors x are 1 and $p - 1 \equiv -1 \bmod p$, and none others, because if

$$x^2 \equiv 1 \bmod p$$

then

$$x^2 - 1 \equiv (x - 1)(x + 1) \equiv 0 \bmod p.$$

In other words, p divides $(x - 1)(x + 1)$.

But then p divides $x - 1$ or p divides $x + 1$ by the prime divisor property, hence

$$x \equiv 1 \mod p \quad \text{or} \quad x \equiv -1 \bmod p,$$

as claimed.

Thus the product $p - 1! \equiv -1 \bmod p$, as needed.

Theorem 2.3 (Lagrange's lemma)**.** *A prime $p = 4n + 1$ divides $m^2 + 1$ for some $m \in \mathrm{Z}$.*

Proof. If we apply Wilsons theorem to the prime $p = 4n + 1$ we get

$$-1 \equiv 1 \text{ x } 2 \text{ x } 3 \text{ x} \ldots \text{x } 4n \bmod p.$$

Now observe that

$$\begin{aligned} &1 \text{ x } 2 \text{ x } 3 \text{ x } \ldots \text{ x } 4n \bmod p \\ \equiv\ &(1 \text{ x } 2 \text{ x } \ldots \text{ x } 2n) \text{ x } ((2n + 1)(2n + 2) \text{ x } \ldots \text{ x } (4n)) \bmod p \\ \equiv\ &(1 \text{ x } 2 \text{ x } \ldots \text{ x } 2n) \text{ x } ((-2n) \text{ x } \ldots \text{ x } (-2) \text{ x } (-1)) \bmod p, \end{aligned}$$

the last congruence holds since

$$2n + 1 \equiv -2n \bmod p,$$

$$2n + 2 \equiv -2n + 1 \bmod p,$$

$$\ldots$$

$$4n \equiv -1 \bmod p,$$

remembering that $p = 4n + 1$.

This is in turn congruent to

$$(1 \text{ x } 2 \text{ x } \ldots 2n))^2(-1)^{2n} \mod p$$

$$\equiv (1 \text{ x } 2 \text{ x } \ldots \text{x } 2n))^2 \qquad \mod p$$
$$\equiv -1 \mod p.$$

Taking $m = (2n)!$ we get $m^2 \equiv -1 \mod p$. That is, p divides $m^2 + 1$.

Definition 2.4. The *norm* of Z[**i**] is the function from Z[**i**] to Z defined as

$$\text{norm}(a + b\mathbf{i}) = |a + b\mathbf{i}|^2 = a^2 + b^2.$$

The norm is multiplicative, hence if

$$\gamma = \alpha\beta \qquad \text{for } \gamma, \alpha, \beta \in \text{Z}[\mathbf{i}],$$

then

$$\text{norm}(\gamma) = \text{norm}(\alpha)\text{norm}(\beta).$$

Definition 2.5. A *Gaussian prime* is a Gaussian integer that is not the product of Gaussian integers of smaller norms.

Example 2.6. $\alpha = 4 + \mathbf{i}$ is a Gaussian prime because

$$\text{norm}(4 + \mathbf{i}) = 16 + 1 = 17,$$

which is a prime in Z.

Hence α is not the product of Gaussian integers of smaller norm, because no such norms divide 17.

Remark 2.7. In the following proof we will use the important fact that the set of Gaussian integers Z[**i**] satisfies the unique factorization property. This is implicit in our assertion that a Gaussian prime has the Gaussian prime divisor property.

The idea of the proof is to study the geometry of Z[**i**] as a lattice in C, and show that the norm on this lattice defines a Euclidean norm, that is to say, a norm with respect to which we can perform the usual Euclidean algorithm. The details are omitted.

Theorem 2.8 (Fermat's two square theorem)**.** *If* $p = 4n + 1$ *is prime in* Z*, then*

$$p = a^2 + b^2 \qquad \text{for some} \qquad a, b \in \text{Z}.$$

Proof. Given p, let m be such that p divides $m^2 + 1$, as in Lagrange's lemma (Theorem 2.3). In Z[**i**], $m^2 + 1$ has the factorization

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

And, even though p divides $m^2 + 1$, p does not divide $m - \mathbf{i}$ or $m + \mathbf{i}$ because the division does not yield a Gaussian integer.

Therefore, by the Gaussian prime divisor property, it follows that p is not a Gaussian prime.

Therefore, it factorizes in Z[**i**]:

$$p = (a + b\mathbf{i})z,$$

where $a + b\mathbf{i}$ and z are Gaussian integers with norm less than the norm p^2 of p.

Taking conjugates of both sides we get

$$p = (a - b\mathbf{i})\bar{z},$$

since p is real and hence p is equal to its conjugate.

Multiplying these two expressions for p yields

$$p^2 = (a - b\mathbf{i})(a + b\mathbf{i})z\bar{z}$$

$$= (a^2 + b^2)|z|^2,$$

where both $a^2 + b^2$ and $|z|^2$ are greater than 1.

But the only such factorization of p^2 is p x p, hence $p = a^2 + b^2$.

Remark 2.9. This theorem has an easy converse:
If $p = 4n + 3$ is a prime in Z*, then p cannot be written as a sum of two squares.*
This is clear since

$a \equiv 0$ or $2 \mod 4 \Rightarrow a^2 \equiv 0 \mod 4$ and $b \equiv 1$ or $3 \mod 4 \Rightarrow b^2 \equiv 1 \mod 4$,

so any square is congruent to 0 or 1 mod 4, hence $p \equiv 3 \mod 4$ cannot be a sum of two squares.

The remaining case of $p = 2$ needs to be treated separately but is trivial.

In fact, we can derive a complete characterization of integers that are sums of two squares:

Corollary 2.10 (Fermat's two square theorem, second version)**.** *A natural number n can be written as a sum of two squares if and only if*

$$n = p^{2\alpha_1}p^{2\alpha_2} \ldots p^{2\alpha_k} q^{2\beta_1+1}q^{2\beta_2+1} \ldots q^{2\beta_l+1}$$

where all the p_i, q_j are prime, and no q_j is congruent to 3 mod 4.

Proof. This follows immediately from the unique factorization property of Z[**i**] and the fact that norm is multiplicative.

3. Lagrange's Four Square Theorem

Theorem 3.1 (Existence of prime factorization)**.** *Each natural number n can be written as the product of primes,*

$$n = p_1p_2p_3 \ldots p_k.$$

Proof. If n itself is a prime there is nothing to do.

If not, $n = ab$ for some smaller a, b. If a or b is not prime we split it into smaller factors, and so on. Since natural numbers cannot decrease forever, we eventually get a factorization

$$n = p_1p_2p_3 \ldots p_k$$

in which no p_i is a product of smaller numbers, hence prime.

Definition 3.2. We define the *quaternions* to be the matrices

$$\begin{bmatrix} a + b\mathbf{i} & c + d\mathbf{i} \\ -c + d\mathbf{i} & a - b\mathbf{i} \end{bmatrix},$$

with $a, b, c, d \in$ R.

The set of quaternions is denoted by H in honor of W. Hamilton who discovered them (possibly also to avoid confusion with the rationals).

It is however more common to write a quaternion in the form $a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$ with the famous relations that Hamilton discovered and cut on the Brougham bridge in Dublin:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1.$$

Just as for the complex numbers, there is a conjugation on H:

$$\overline{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}} := a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}.$$

Then the norm is defined in a similar fashion

$$\begin{aligned}\text{norm}(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) &:= (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})\overline{(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})} \\ &= a^2 + b^2 + c^2 + d^2.\end{aligned}$$

From this expression it is clear that the norm takes values in R.

The following identity of Euler follows immediately:

Corollary 3.3 (Euler's Four Square Identity)**.**

$$\begin{aligned}&(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) \\ &= (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 \\ &\quad + (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2.\end{aligned}$$

Because of this identity, the proof of the four square theorem is reduced to the corresponding statement for each prime.

Note that

$$2 = 0^2 + 0^2 + 1^2 + 1^2,$$

so it remains to prove that every odd prime is the sum of four integer squares.

This is done with the help of a simple lemma:

Lemma 3.4. *If $p = 2n + 1$, then there are $l, m \in \mathbb{Z}$ such that p divides $1 + l^2 + m^2$.*

This lemma is comparable to Lagrange's lemma, in the previous proof, but much easier.

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

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

And

$$x + y \not\equiv 0 \bmod p \text{ since } 0 < x + y < p.$$

Thus the $n + 1$ numbers $l = 0, 1, 2, \ldots, n$ give $n + 1$ incongruent values of l^2 mod p.

Similarly, the numbers $m = 0, 1, 2, \ldots, n$ give $n + 1$ incongruent values of m^2, hence of $-m^2$, and hence of $-1- m^2$.

But only $2n + 1$ incongruent values exist mod p.

Therefore, for some l and m we have

$$l^2 \equiv 1 - m^2 \qquad \bmod p,$$

or equivalently,

$$p \quad \text{divides} \quad 1 + l^2 + m^2.$$

Definition 3.5. A *Hurwitz integer* is a quaternion whose components are either all integers or all half-integers (halves of an odd integer; a mixture of integers and half-integers is not allowed). The set of all Hurwitz quaternions is

$$H = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathrm{H} : a, b, c, d \in \mathrm{Z} \text{ or } \mathrm{Z} + ½ \}$$

A Hurwitz integer is defined to be a *Hurwitz prime* if its H-norm is a prime number $p \in \mathrm{Z}$.

Note that the norm on H restricts to a Z-valued function on the set of Hurwitz integers. Therefore the definition of a Hurwitz prime makes sense, and is completely analogous to Z[**i**].

Remark 3.6. The correct definition of Hurwitz integers includes more quaternions than the naive guess Z[**i**, **j**, **k**] (the set of quaternions with $a, b, c, d \in \mathrm{Z}$).

This accounts for the fact that the division property fails for Z[**i**, **j**, **k**] We can consider them integers because the sum, difference, and product of two Hurwitz integers is again a Hurwitz integer, and also the norm of a Hurwitz integer is an ordinary integer.

Of particular importance is the prime divisor property of Hurwitz integers. The proof is again similar to the Gaussian integers, but involves more geometry and is also omitted.

One should compare the Hurwitz integers to the ring of integers of $\mathrm{Q}(\sqrt{d})$ for $d \equiv 1 \bmod 4$, which also includes certain half-integer terms. In fact using such rings of integers we can prove representability results for certain quadratic forms that are related to their norms.

Theorem 3.7 (Lagrange's four square theorem)**.** *Every natural number is the sum of four squares.*

Proof. As demonstrated, it remains to prove the theorem for any odd prime p, which we have just shown to divide a number $1 + l^2 + m^2$. We factorize $1 + l^2 + m^2$ into the product of Hurwitz integers

$$(1 - l\mathbf{i} - m\mathbf{j})(1 + l\mathbf{i} + m\mathbf{j}),$$

and utilize the prime divisor property of Hurwitz integers.

If p is a Hurwitz prime, then p divides $1 - l\mathbf{i} - m\mathbf{j}$ or p divides $1 + l\mathbf{i} + m\mathbf{j}$. But neither conclusion is true as in the previous theorem because neither division is a Hurwitz integer.

It follows now that no ordinary prime number in Z remains prime as a Hurwitz integer, hence we can write $p = \alpha\beta$ with α, β both Hurwitz integers, such that

$$\mathrm{norm}(\alpha) < \mathrm{norm}(p) \quad \text{and} \quad \mathrm{norm}(\beta) < \mathrm{norm}(p).$$

The norms of p, α, β are nonnegative integers such that

$$p^2 = \mathrm{norm}(p) = \mathrm{norm}(\alpha\beta) = \mathrm{norm}(\alpha)\mathrm{norm}(\beta).$$

But the norm has only two factors, both p. Therefore, p is the sum of four squares:

$$p = \mathrm{norm}(\alpha) = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2,$$

where

$$\alpha = \alpha_1 + \alpha_2\mathbf{i} + \alpha_3\mathbf{j} + \alpha_4\mathbf{k}.$$

If the α_i are all integers then we are done. Therefore we assume that all the α_i are half-integers.

A Hurwitz integer α with half-integer coordinates can always be written in the form

$$\alpha = \omega + a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k},$$

where a, b, c, d are even integers, by a suitable choice of signs in the Hurwitz integer

$$\omega = \frac{\pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k}}{2}$$

The norm of ω is 1, so that multiplication with its conjugate is 1.

Now suppose $p = a^2 + b^2 + c^2 + d^2$ for an ordinary prime p, as in the last paragraph, and that a, b, c, d are half-integers. We first write

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

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

where a, b, c, d are even and ω is as above (ω denoting its conjugate), so $\omega\omega = 1$. Next we insert $1 = \omega\omega$ between the (conjugate) factors just found, and in this way obtain new conjugate factors of p,

$$p = (\omega + a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})\omega\omega(\omega + a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}).$$

In the first factor, ω plus the even integer terms times ω gives 1 plus integer terms, hence it is

$$A + B\mathbf{i} + C\mathbf{j} + D\mathbf{k} \text{ for some } A, B, C, D \in \mathbb{Z}.$$

The second factor is its conjugate, hence

$$p = A^2 + B^2 + C^2 + D^2 \qquad \text{for some} \quad A, B, C, D \in \mathbb{Z}.$$

Remark 3.8. Note that this result is best possible in the following sense:
There are (infinitely many) numbers not expressible as a sum of three squares.
To prove this we observe the following:

$$A \equiv 0 \text{ or } 4 \mod 8 \Rightarrow a^2 \equiv 0 \mod 8, \quad b \equiv 2 \text{ or } 6 \mod 8 \Rightarrow b^4 \equiv 1 \mod 8,$$

$$\text{and } c \equiv 1 \text{ or } 3 \text{ or } 5 \text{ or } 7 \mod 8 \Rightarrow \equiv 1 \mod 8.\ c^2$$

Therefore a number of the form 7 mod 8 cannot be written as a sum of three squares.

Acknowledgments. I would like to thank my mentor, Shuyang Cheng, for his help with the preparation and editing of this paper. It would not have been possible otherwise.

References

[1] Stillwell, John. Elements of Number Theory: With 35 Figures. New York: Springer, 2003. Print.