The goal of this document is to classify the integers which equal the sum of two squares. This classification was first done by Albert Girard, published in 1634 after his death. It was first proven in 1740 by Euler.

Remarkably, this proof depends crucially on certain arithmetic properties of complex numbers; we assume the reader has some basic familiarity with complex numbers, and with modular arithmetic. While we will not require any difficult mathematics, we will introduce a significant amount of notation and terminology not seen at a high school level.

We begin by classifying which prime numbers are equal to the sum of two squares; this result is known as Fermat's theorem on sums of two squares. We will then use this result to show how to classify any integer given its factorization into primes.

1 Terminology

We introduce some basic terminology from ring theory which will prove useful in this document.

A *ring* is a set R of numbers which can be added or multiplied (that is, if $a, b \in R$ then $a + b, ab \in R$). We assume that addition and multiplication are associative, commutative, distributive, and that there is a zero and one in the ring.

In this document we will work with four rings:

- the ring of integers, $\mathbb{Z}$
- the ring of Gaussian integers $\mathbb{Z}[i]$, which are complex numbers of the form $a+bi$ where a and b are integers
- for some ring R, the ring $R[x]$ of polynomials whose coefficients are elements of R
- the ring $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n

The ring of integers modulo n is the same as the ordinary integers except that two integers are considered equivalent in $\mathbb{Z}/n\mathbb{Z}$ if their difference is divisible by n (that is, if they have the same remainder modulo n). For example, in $\mathbb{Z}/5\mathbb{Z}$, $3 = 8$ but $3 \neq 7$. This can lead to confusion if it is ambiguous whether we are working in $\mathbb{Z}$ or in $\mathbb{Z}/n\mathbb{Z}$, so we sometimes write $a \equiv b \ \ (n)$ to explicitly mean that the integers a and b are equal in $\mathbb{Z}/n\mathbb{Z}$.

The ring $\mathbb{Z}/n\mathbb{Z}$ has exactly n elements.

We write $a \mid b$ in some ring R (said a *divides* b) if there exists $k \in R$ such that $b = ak$. We say a is a *unit* if $a \mid 1$. Note that if $a \mid b$ and b is a unit then a is a unit.

We say p is *irreducible* if p is not a unit and whenever $p = ab$ then either a or b is a unit. We say that p is *prime* if p is not a unit and whenever $p \mid ab$ then either $p \mid a$ or $p \mid b$. When discussing primes in the integers $\mathbb{Z}$ we only ever consider positive primes.

It is easy to prove that any prime element is irreducible; for if p is prime and $p = ab$, then $p \mid ab$, so $p \mid a$ (say), so $ab \mid a$, so $b \mid 1$ and b is a unit. However there exist rings where there are irreducible elements which are not prime.

Equivalent to p (a non-unit integer) being prime is that whenever $ab = 0$ in Z/pZ, then either $a = 0$ or $b = 0$, which is to say that Z/pZ does not have any *zero divisors*. This is just a different way of expressing the definition of primality.

2 Why modulo 4?

The next section is devoted to proving the claim that whenever p is a prime with $p \equiv 1 \ (4)$, it follows that $p = a^2 + b^2$ for some integers a and b. Before we dive into the technical details of the proof, let us briefly discuss why it is interesting to consider $a^2 + b^2$ in modular arithmetic, in particular modulo 4.

Before we consider $a^2 + b^2$, just consider squares a^2. Can we know whether some number n is a perfect square by knowing its remainder mod k? (A number congruent to a perfect square mod k is called a *quadratic residue*.) Sometimes, we can, because some remainders are impossible. So let us make a list of all possible quadratic residues mod k, which is to say which numbers in the ring Z/kZ are perfect squares. Since $0, 1, \ldots, k-1$ is a complete list of the numbers in Z/kZ, therefore $0^2, 1^2, \ldots, (k-1)^2$ is a complete list of all the perfect squares.

However this list has some duplicates, because $a^2 = (-a)^2$, so most squares can be reached in (at least) two different ways. For example, when $k = 7$ the squares are $0^2, 1^2, 2^2$, and 3^2 as $4 = -3, 5 = -2$, and $6 = -1$, so the remaining squares are duplicates of ones already listed. In general we see that there are fewer than k quadratic residues mod k, so for some numbers n we can tell that it is not a perfect square if it is not a quadratic residue mod k for some k.

So if we are given a number n and know its remainder modulo k, if it does not equal a quadratic residue then we know n cannot be a perfect square. Let us look at some quadratic residues for small moduli:

0	mod 1
$0, 1$	mod 2
$0, 1$	mod 3
$0, 1$	mod 4
$0, 1, 4$	mod 5
$0, 1, 3, 4$	mod 6
$0, 1, 2, 4$	mod 7
$0, 1, 4$	mod 8
$0, 1, 4, 7$	mod 9
$0, 1, 4, 5, 6, 9$	mod 10
$0, 1, 3, 4, 5, 9$	mod 11

So for example, if $x \equiv 3(7)$ then we know $x \neq a^2$ for any a.

Now we ask if we can perform the same procedure to know whether a number n can be written in the form $a^2 + b^2$ for some a and b, by examining the remainder of n mod some choice of k. Once we know the quadratic residues modulo k, we can add together any two quadratic residues modulo k and get a list of all possible remainders of numbers of the form $a^2 + b^2$. This may allow us to eliminate the possibility that $n = a^2 + b^2$ for some n by looking and its remainder modulo some k. We find that the possible remainders of $a^2 + b^2$ modulo k are:

0	mod 1
$0, 1$	mod 2
$0, 1, 2$	mod 3
$0, 1, 2$	mod 4
$0, 1, 2, 3, 4$	mod 5
$0, 1, 2, 3, 4, 5$	mod 6
$0, 1, 2, 3, 4, 5, 6$	mod 7
$0, 1, 2, 4, 5$	mod 8
$0, 1, 2, 4, 5, 7, 8$	mod 9
$0, 1, 2, 3, 4, 5, 6, 7, 8, 9$	mod 10
$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$	mod 11

It looks like for most k, there are not very many (if any) remainders that are impossible. In fact, it turns out that only $k = 4$ is useful this way! In fact, if k is not a multiple of 4, then for any remainder r relatively prime to k, there are numbers a, b with $a^2 + b^2 \equiv r \pmod{k}$. (This is a consequence of Dirichlet's theorem, which is a very challenging theorem not proven until 1837.) Since we are first interested in what *primes* p are of the form $a^2 + b^2$, only the remainders relatively prime to k are useful (since p is always relatively prime to k when $k < p$), so the only modulo that helps is $k = 4$.

We see that $a^2 + b^2$ is never congruent to 3 modulo 4, so if $p \equiv 3 \pmod{4}$ then p does not equal $a^2 + b^2$ for any a, b (and this does not require that p is prime in any way). The converse (that if p is a prime and $p \equiv 1 \pmod{4}$ then $p = a^2 + b^2$) is always true, does require that p is prime, and is the subject of the next section.

3 Fermat's theorem on sums of two squares

Lemma 1 (polynomial division with remainder)**.** *Let R be a ring and f be in $R[x]$ (that is, f is a polynomial with coefficients in R). Let $\alpha \in R$. Then there exists $g \in R[x], r \in R$ (called the* quotient *and* remainder*) such that*

$$f(x) = g(x)(x - \alpha) + r.$$

Proof. f is a linear combination of monomials x^k, each of which can be written in the desired form:

$$x^k = (x^{k-1} + \alpha x^{k-2} + \alpha^2 x^{k-3} + \cdots + \alpha^{k-2} x + \alpha^{k-1})(x - \alpha) + \alpha^k,$$

□

Lemma 2 (Lagrange's Theorem)**.** *For a prime p, a nonzero polynomial $f(x)$ has at most* $\deg f$ *roots in Z/pZ.*

Proof. Here $\deg f$ is the *degree* of f, the highest power of x that appears with a nonzero coefficient in f.

Suppose $\alpha \in Z/pZ$ is some root of f. Then by the lemma we have

$$f(x) = g(x)(x - \alpha) + r$$

for some quotient g and remainder r. In fact, evaluating both sides at $x = \alpha$, we see that $r = f(\alpha) = 0$, so

$$f(x) = g(x)(x - \alpha).$$

Now if $\beta \neq \alpha$ is any other root of f, then plugging in $x = \beta$ we see that $(\beta - \alpha)g(\beta) = 0$ in Z/pZ. Since p is prime therefore $g(\beta) = 0$, so β is a root of g. Therefore f has at most one more root than g does, and $\deg f = 1 + \deg g$, so by induction f has at most $\deg f$ roots. □

Note that this proof works for polynomials over any ring R without zero divisors, such as the integers $\mathbb{Z}$, the rationals, the reals, and the complex numbers.

Lemma 3. *If p is prime and $p \equiv 1 \pmod 4$, then there exists n such that $p \mid n^2 + 1$.*

Proof. First we show that $p \mid a^p - a$ for every integer a. (This is known as Fermat's little theorem.) If we assume the binomial theorem, we can determine this immediately by calculating $(a + 1)^p \equiv a + 1 \pmod p$ and inducting on a. However to avoid using the binomial theorem, we give a somewhat longer proof of the claim.

Consider the nonzero elements $U = \{1, 2, \ldots, p - 1\}$ in $\mathbb{Z}/p\mathbb{Z}$ and choose some $a \in U$. Consider the sequence of powers of a, that is $1, a, a^2, \ldots$, which are elements of U. Since U is finite this sequence must repeat so there is some $a^i = a^j$ with $j > i$. Then $a^i(a^{j-i} - 1) = 0$ (in $\mathbb{Z}/p\mathbb{Z}$), but $a^i \neq 0$ and p is prime, so $a^{j-1} = 1$, which is to say that some positive power of a is equal to 1. Let k be the smallest positive number with $a^k = 1$.

Now for any $b, c \in U$ we say that b and c are "equivalent" if $b = ca^i$ for some i, or vice versa. Clearly the numbers equivalent to b are simply $b, ba, \ldots, ba^{k-1}$; since $a^k = 1$, any further powers of a just repeats numbers we have already seen. Those k numbers are distinct because the numbers $1, \ldots, a^{k-1}$ are distinct and they must remain distinct when multiplied by b because p is prime.

We partition U into collections of numbers which are equivalent to each other. We've found that each collection of equivalent numbers contains exactly k distinct elements, so k must divide the size of U, which is $p - 1$. Therefore

$$a^{p-1} = (a^k)^{(p-1)/k} = 1^{(p-1)/k} = 1$$

or $a^p = a$ in $\mathbb{Z}/p\mathbb{Z}$ for any $a \in U$. Clearly this is also true when $a = 0$, so this holds for all $a \in \mathbb{Z}/p\mathbb{Z}$.

Returning to the integers $\mathbb{Z}$, this says that $a^p \equiv a \pmod p$ for any integer a, which is what we wanted to show. This proof effectively proved what is called Lagrange's theorem in group theory (unrelated to Lemma 2), which implies Euler's theorem, which implies Fermat's little theorem; so in fact we've proven quite a bit more than necessary.

Now that we know that $a^p = a$ for all $a \in \mathbb{Z}/p\mathbb{Z}$, consider the polynomial $x^p - x$ in $\mathbb{Z}/p\mathbb{Z}[x]$; we see that it has all p roots (namely, $0, 1, \ldots, p-1$). We can factor the polynomial as

$$x^p - x = x(x^{p-1} - 1) = x\left(x^{(p-1)/2} - 1\right)\left(x^{(p-1)/2} + 1\right).$$

Lemma 2 gives us an upper bound on how many roots each of the terms on the right can have. But we know the term on the left has p roots, which equals its degree and so is the maximum possible, so therefore each term on the right must have their maximum as well. In particular $x^{(p-1)/2} + 1$ has at least one root in $\mathbb{Z}/p\mathbb{Z}$, call it a. Let

$$n = a^{(p-1)/4},$$

so that $n^2 = a^{(p-1)/2} = -1$ in $\mathbb{Z}/p\mathbb{Z}$. Therefore $p \mid n^2 + 1$ in the integers. □

Note that this lemma is the same as saying that -1 is a quadratic residue modulo an odd prime p if and only if $p \equiv 1 \pmod 4$.

To continue this proof we need to discuss complex numbers of the form $a + bi$ where a and b are integers. These numbers are called the Gaussian integers, and the collection of all Gaussian integers is written $\mathbb{Z}[i]$.

We define a *norm* on the Gaussian integers by

$$N(\alpha) = \alpha\overline{\alpha}$$

where $\overline{\alpha}$ is the complex conjugate of α. If $\alpha = a + bi$ then $\overline{\alpha} = a - bi$ and $N(\alpha) = a^2 + b^2$.

For any Gaussian integers $\alpha, \beta \in \mathbb{Z}[i]$,

$$N(\alpha\beta) = \alpha\beta\overline{\alpha}\overline{\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta),$$

which is to say that the norm is *multiplicative*.

The units of $\mathbb{Z}[i]$ are $1, -1, i, -i$, which are exactly the numbers with norm 1.

Recall we defined "prime" and "irreducible", and proved that every prime element is irreducible. The converse is not always true. We say that a ring R is a *unique factorization domain* (UFD) if every irreducible element is prime. Equivalently, a UFD is a ring where every element can be uniquely (up to units) written as a product of irreducible numbers. (The proof that these definitions are equivalent is easy.)

We need an additional fact which we will not prove: $\mathbb{Z}$ and $\mathbb{Z}[i]$ are UFDs.

The fact that $\mathbb{Z}$ is a UFD is simply the Fundamental Theorem of Arithmetic, an elementary fact that every integer can be uniquely factored into irreducible numbers. The proof that $\mathbb{Z}[i]$ is a UFD is almost identical to the proof for $\mathbb{Z}$ so we take both claims without proof.

The key to the proof concerns understanding the relationship between the numbers that are prime in $\mathbb{Z}$ and prime in $\mathbb{Z}[i]$. Now that we know that irreducibles are prime in both rings, we can proceed.

Theorem 4 (Fermat's theorem on sums of two squares)**.** *If p is prime, then there exists a, b such that $p = a^2 + b^2$ if and only if $p = 2$ or $p \equiv 1 (4)$.*

Proof. If $p = 2$ then $p = 1^2 + 1^2$. If $p \equiv 3 \pmod 4$ we argued before that it is impossible that $p = a^2 + b^2$ (this does not even require that p is prime). All that remains is to show that if $p \equiv 1 \pmod 4$ then there exist the required a, b.

By Lemma 3, there exists n such that $p \mid n^2 + 1$. Then, working in $\mathbb{Z}[i]$,

$$p \mid (n + i)(n - i).$$

If p were prime in $\mathbb{Z}[i]$ then we would have either $p \mid (n + i)$ or $p \mid (n - i)$. Since p is an integer, if $p \mid a + bi$ we must have $p \mid a$ and $p \mid b$, so therefore $p \mid 1$ which contradicts that p is prime in $\mathbb{Z}$ and therefore not a unit. Therefore p is not prime in $\mathbb{Z}[i]$.

As $\mathbb{Z}[i]$ is a UFD and p is not prime in $\mathbb{Z}[i]$, therefore it is also not irreducible, so $p = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[i]$ that are not units. Therefore

$$p^2 = N(p) = N(\alpha)N(\beta).$$

Since α and β are not units, therefore $N(\alpha)$ and $N(\beta)$ are not 1, but their product is p^2, so $N(\alpha) = N(\beta) = p$. Write $\alpha = a + bi$. Then $p = N(\alpha) = a^2 + b^2$. □

4 Classification of sums of squares

Having determined which prime numbers can be expressed as a sum of two squares, we can characterize all integers in terms of their factorization.

Lemma 5. *If a, b are integers that are both a sum of two squares, then so is ab.*

Proof. An integer is a sum of two squares if and only if it is the norm of some Gaussian integer. So write $a = N(\alpha), b = N(\beta)$, and therefore $ab = N(\alpha\beta)$ is also a sum of two squares. Note that also $ab = N(\alpha\overline{\beta})$ so generally speaking ab can be written as a sum of two squares more than one way. □

It follows from this that if n factors as $n = p_1^{a_1} \cdots p_k^{a_k}$ where a_i is even whenever $p_i \equiv 3 \pmod 4$, then n is a sum of two squares. It remains to be shown the converse, that all sums of two squarse are of this form.

Lemma 6. *If p is prime in $\mathbb{Z}$ and $p \equiv 3 \pmod 4$, then p is a prime in $\mathbb{Z}[i]$.*

Proof. Suppose otherwise; since $\mathbb{Z}[i]$ is a UFD, then p would be reducible as $p = \alpha\beta$ for non-units $\alpha, \beta \in \mathbb{Z}[i]$. Then $N(\alpha)N(\beta) = p^2$ so $N(\alpha) = p$, which is impossible because the norm is a sum of two squares and can never be congruent to 3 modulo 4. □

Theorem 7. *If n is a positive integer then n is a sum of two squares if and only if it factors as $n = p_1^{a_1} \cdots p_k^{a_k}$ where a_i is even whenever $p_i \equiv 3 \pmod 4$.*

Proof. We have already shown one direction, so it only remains to show the other. Suppose n is a sum of two squares, so $n = N(\alpha) = \alpha\overline{\alpha}$ for some $\alpha \in \mathbb{Z}[i]$. For each prime $p \equiv 3 \pmod 4$ we need to show that p divides n evenly many times. Since $\mathbb{Z}[i]$ is a UFD, we can look at the unique factorization of α into primes; as p is prime in $\mathbb{Z}[i]$, suppose p appears m times in the factorization of α. Then $\overline{p} = p$ appears m times in the factorization of $\overline{\alpha}$, and thus a total of $2m$ times in the factorization of n in $\mathbb{Z}[i]$ and in $\mathbb{Z}$. □