2. Sums of squares

We consider the question of when we can write an integer n as a sum of two squares, that is, we consider for which integers n we can solve the equation

$$x^2 + y^2 = n,$$

where x and y are integers.

This question will be relatively easy to solve, due to the following identity:

Lemma 2.1. *If a, b, c and d are reals then*

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

In particular the set of integers which are the sum of two squares is closed under multiplication.

Proof. Of course we can check this formally (so that it holds over any commutative ring). But we can also use complex numbers

$$\begin{aligned}
(a^2 + b^2)(c^2 + d^2) &= (a + bi)(a - bi)(c + di)(c - di) \\
&= (a + bi)(c + di)(a - bi)(c - di) \\
&= [ac - bd + i(bc + ad)][ac - bd - i(bc + ad)] \\
&= (ac - bd)^2 + (ad + bc)^2.
\end{aligned}$$

□

Definition 2.2. *We say that a solution (u, v) to*

$$x^2 + y^2 = n,$$

*is **primitive** if $(u, v) = 1$.*

Proposition 2.3. *If n has a primitive representation then -1 is a quadratic residue of n.*

In particular if $p \equiv 3 \mod 4$ and $p|n$ then and n is a sum of squares then $n = p^{2k}m$ where m is coprime to p and if $x^2 + y^2 = n$ then we may write $x = p^k x'$ and $y = p^k y'$.

Proof. Let

$$u^2 + v^2 = n$$

be a primitive representation and let p be a prime divisor of n. Then p does not divide u and so we may find w such that $wu \equiv 1 \mod p$. Multiplying the equation above by w^2 and reducing modulo p we get

$$1 + (wv)^2 \equiv 0 \mod p.$$

Thus -1 is a quadratic residue of p.

Suppose that p is odd. If we apply Newton-Raphson approximation to the function $f(x) = x^2$, see lecture 12 from Math 104A, it follows that -1 is a quadratic residue of p^e for any natural number e.

If p is even then note that both u and v are odd. In this case $u^2 \equiv 1 \mod 4$ so that $n \equiv 2 \mod 4$. But then n is not divisible by 4.

Now we may apply the Chinese remainder theorem to conclude that -1 is a quadratic residue of n.

Now suppose that $p \equiv 3 \mod 4$. Then -1 is not a quadratic residue modulo p and so no integer divisible by p has a primitive representation. Suppose that $n = p^h m$ where m is coprime to p. Suppose that

$$u^2 + v^2 = n$$

and let $d = (u, v)$. Then we may write $u = du_1$ and $v = dv_1$ and $d^2|n$ so that $n = d^2 N$, $N \in \mathbb{Z}$. It follows that

$$u_1^2 + v_1^2 = N$$

where $(u_1, v_1) = 1$. By what we already proved N is coprime to p. Thus if $d = p^k e$, where e is coprime to d, then $h = 2k$. $\square$

Proposition 2.4. *Let $n > 1$ be a natural number of which -1 is a quadratic residue. Then to each solution u of*

$$u^2 \equiv -1 \mod n,$$

there corresponds a unique pair of integers x and y such that

$$n = x^2 + y^2, \quad x > 0, \quad y > 0, \quad (x, y) = 1 \quad \textit{and} \quad y \equiv ux \mod n,$$

and vice-versa.

Proof. Suppose we are given u. By (1.2), applied to $\lambda = \sqrt{n}$ and $a = u$, we may find r and s such that

$$us \equiv r \mod n \qquad 0 < s < \sqrt{n} \qquad \text{and} \qquad |r| \leq \sqrt{n}.$$

If $r > 0$ then let $x = s$ and $y = r$. If $r < 0$ then note that $s \equiv -ur \mod n$ and let $x = -r$ and $y = s$. Either way,

$$x^2+y^2 \equiv 0 \mod n \quad 0 < x \leq \sqrt{n}, \quad 0 < y \leq \sqrt{n}, \quad \text{and} \quad y \equiv ux \mod n$$

and at most one of x and y is equal to $\sqrt{n}$. Hence

$$\begin{aligned} 0 < x^2 + y^2 &= tn \\ &< 2n. \end{aligned}$$

It follows that

$$x^2 + y^2 = n.$$

By assumption there are integers k and l such that $u^2 + 1 = kn$ and $y = ux + ln$. We have

$$\begin{aligned} n &= x^2 + y^2 \\ &= x^2 + (ux + ln)y \\ &= x^2 + ux(ux + ln) + lny \\ &= x^2(1 + u^2) + uxln + lny \\ &= xn(kx + ul) + lny, \end{aligned}$$

so that $x(kx + ul) + ly = 1$. It follows that $(x, y) = 1$ and so

$$n = x^2 + y^2, \quad x > 0, \quad y > 0, \quad (x, y) = 1 \quad \text{and} \quad y \equiv ux \mod n.$$

This establishes existence.

Now suppose that

$$n = X^2 + Y^2, \quad X > 0, \quad Y > 0, \quad (X, Y) = 1 \quad \text{and} \quad Y \equiv uX \mod n.$$

We have

$$\begin{aligned} n^2 &= (x^2 + y^2)(X^2 + Y^2) \\ &= (xX + yY)^2 + (xY - Xy)^2. \end{aligned}$$

It follows that $0 < xX + yY \leq n$. But we have

$$\begin{aligned} xX + yY &\equiv xX + u^2 xX \\ &\equiv 0 \mod n. \end{aligned}$$

Therefore $xX + yY = n$ and so $xY - Xy = 0$. As $(x, y) = (X, Y) = 1$ it follows that $x = X$ and $y = Y$. This establishes uniqueness.

Now suppose that we have integers x and y such that

$$n = x^2 + y^2, \quad x > 0, \quad y > 0, \quad (x, y) = 1 \quad \text{and} \quad y \equiv ux \mod n.$$

As $(x, n) = 1$ the last condition uniquely determines u. As

$$\begin{aligned} 0 &\equiv x^2 + y^2 \\ &\equiv x^2(1 + u^2) \mod n, \end{aligned}$$

we must have

$$u^2 \equiv -1 \mod n. \qquad \square$$

Definition-Theorem 2.5. *The number $p_2(n)$ of primitive representations of $n > 1$ as a sum of two squares is four times the number of solutions of the congruence $u^2 \equiv -1 \mod n$:*

$$p_2(n) = \begin{cases} 0 & \text{if } 4 | n \text{ or some prime } p \equiv 3 \mod 4 \text{ divides } n. \\ 4 \cdot 2^s & \text{if } 4 \not| n, \text{ no prime } p \equiv 3 \mod 4 \text{ divides } n, \end{cases}$$

where s is the number of odd prime divisors of n.

Proof. If $x^2 + y^2 = n$ and $(x, y) = 1$ then $xy \neq 0$. Note that $(\pm x, \pm y)$ gives four different representations, of which one satisfies the properties of (2.4). $\square$

Corollary 2.6. *A prime $p \not\equiv 3 \mod 4$ can be uniquely represented, up to order and sign, as a sum of two squares.*

Conversely, suppose that N is odd. If N has a unique representation, up to order and sign, and this representation is primitive, then N is prime.

If N has only one primitive representation then N is a power of a prime congruent to one modulo 4.

Proof. If $p = 2$ then $p_2(2) = 4$ and the four different representations $(\pm 1)^2 + (\pm 1)^2$ are the same up to sign. If $p \equiv 1 \mod 4$ then $p_2(p) = 8$. If $a^2 + b^2 = p$ then $(a, b) = 1$. As $p > 2$ it follows that $a \neq b$ and so the eight different primitive representations $(\pm a)^2 + (\pm b)^2$ and $(\pm b)^2 + (\pm a)^2$ are the same up to sign and order.

Now suppose N is odd. If N has a unique primitive representation, up to order and sign, then $s = 1$, so that N is a power p^e of a prime $p \equiv 1 \mod 4$.

Suppose $e > 1$. If $e = 2$ then $p^2 + 0^2$ gives one representation and multiplying a representation of p with itself gives another representation. If $e > 2$ then multiplying representations of lower powers gives more than one representation. $\square$