5. Quadratic forms

5.1 Sums of two squares

In this section, we deal with the question of which positive integers can be written as a sum of squares of two integers. For a sum of squares of integers (so we allow that summands are equal to 0), we will often simply say "sum of squares".

Proposition 5.1. *If positive integers m and n are sums of two squares, then their product $m \cdot n$ is also a sum of two squares.*

Proof: Let $m = a^2 + b^2$ and $n = x^2 + y^2$. Then

$$mn = (ax + by)^2 + (ay - bx)^2 = (ax - by)^2 + (ay + bx)^2, \tag{5.1}$$

so mn can also be written as a sum of two squares. □

Since every integer greater than 1 is a product of prime numbers, the previous proposition suggests that we should first consider which prime numbers can be written as a sum of two squares.

Proposition 5.2. *A prime number p of the form $4k + 3$ is not a sum of two squares. Moreover, if $p \mid (x^2 + y^2)$, then $p \mid x$ and $p \mid y$.*

Proof: Assume that $p \mid (x^2 + y^2)$. Then $x^2 \equiv -y^2 \pmod{p}$. Raising both sides of the congruence to the power $\frac{p-1}{2}$, we obtain

$$x^{p-1} \equiv (-1)^{(p-1)/2} y^{p-1} \pmod{p}.$$

If $p \nmid x$ (which implies $p \nmid y$), then from Fermat's little theorem, it follows that $1 \equiv -1 \pmod{p}$, which is a contradiction. Therefore, $p \mid x$ and $p \mid y$, so the second statement of the proposition is proved. The first statement follows from the second one since x and y have to be relatively prime to p if $p = x^2 + y^2$. So, p cannot be represented as a sum of two squares. □

Proposition 5.3. *If a prime number p divides the sum of two squares x^2+y^2, where $\gcd(x,y)=1$, then p can be represented as a sum of two squares.*

Proof: The so-called *method of descent* is applied in the proof.

Assume that $p\cdot k$ is the least multiple of p which can be represented in the form

$$pk = x^2+y^2, \quad \gcd(x,y)=1.$$

Let $x \equiv a \pmod{p}$, $y \equiv b \pmod{p}$, where $|a|,|b| \le \frac{p}{2}$ (absolutely least residues). Then $a^2+b^2 \equiv x^2+y^2 \equiv 0 \pmod{p}$ and $a^2+b^2 \le \frac{p^2}{4}+\frac{p^2}{4} = p\cdot\frac{p}{2}$. Hence, $1 \le k \le \frac{p}{2}$.

Assume that $k>1$. Let $x \equiv u \pmod{k}$, $y \equiv v \pmod{k}$, $|u|,|v| \le \frac{k}{2}$. Then $u^2+v^2 \equiv x^2+y^2 \equiv 0 \pmod{k}$, so $u^2+v^2 = kl$, for a positive integer l. We have $u^2+v^2 \le \frac{k^2}{2}$, so $1 \le l \le \frac{k}{2} < k$. Let us consider the equality

$$pk^2l = (x^2+y^2)(u^2+v^2) = (xu+yv)^2 + (xv-yu)^2.$$

We have

$$xu+yv \equiv x^2+y^2 \equiv 0 \pmod{k},$$
$$xv-yu \equiv xy-xy \equiv 0 \pmod{k},$$

so there are integers x_0, y_0 such that $xu+yv = x_0k$, $xv-yu = y_0k$. We obtain $pl = x_0^2+y_0^2$. If $\gcd(x_0,y_0)=d$, with $x_0 = dx_1$, $y_0 = dy_1$, then $p\cdot\frac{l}{d^2} = x_1^2+y_1^2$. However, $\frac{l}{d^2} \le l < k$, so we obtained a contradiction to the minimality of k. Hence, $k=1$ (if $k=1$, then $l=0$) and $p = x^2+y^2$. □

Proposition 5.4. *Let p be a prime number of the form $4k+1$. Then there exists a positive integer x such that $p \mid (x^2+1)$.*

Proof: See Theorem 3.14. □

Proposition 5.5. *A prime number p is a sum of two squares if and only if $p=2$ or $p\equiv 1 \pmod{4}$.*

Proof: Directly from Propositions 5.2, 5.4 and 5.3. □

Proposition 5.6. *The representation of a prime number as a sum of two squares is unique (if it exists).*

Proof: Let us assume that $p = a^2+b^2 = c^2+d^2$ for some $a,b,c,d \in \mathbb{Z}$. We can assume that a and c, as well as b and d, are of the same parity. We can rewrite the equality $a^2+b^2=c^2+d^2$ as

$$\frac{a-c}{2}\cdot\frac{a+c}{2} = \frac{d-b}{2}\cdot\frac{d+b}{2}, \quad a\ne c,\ b\ne d.$$

Let $\gcd(\frac{a-c}{2}, \frac{d-b}{2}) = s$ and $\frac{a-c}{2} = st$, $\frac{d-b}{2} = su$. We have $t \cdot \frac{a+c}{2} = u \cdot \frac{d+b}{2}$. Since u and t are relatively prime, we get $\frac{a+c}{2} = uv$, $\frac{d+b}{2} = tv$. Hence, $a = st + uv$ and $b = tv - su$, so $p = a^2 + b^2 = (s^2 + v^2)(t^2 + u^2)$ and we obtained a contradiction with the assumption that p is a prime number. □

Theorem 5.7. *A positive integer n can be represented as a sum of two squares if and only if in its prime factorization, all prime factors of the form $4k + 3$ appear with an even exponent.*

Proof: Necessity follows from Proposition 5.2. Namely, if $p = 4k + 3$ and $p \mid (x^2 + y^2)$, then $p \mid x$ and $p \mid y$. Hence, $p^2 \mid n$, so we can apply the same consideration to $\frac{n}{p^2}$, and we conclude that in the factorization of n, the prime number p appears with an even exponent.

Sufficiency follows from Propositions 5.5 and 5.1. Indeed, n can be written in the form $n = m^2 \cdot n'$, where n' is a product of prime numbers of the form $4k + 1$ (and possibly of prime number 2). From Propositions 5.5 and 5.1, by mathematical induction over the number of factors, it follows that n' is a sum of two squares, $n' = x^2 + y^2$. But then $n = (mx)^2 + (my)^2$. □

Example 5.1. *Let $r_2(n)$ denote the number of representations of n as a sum of squares of two integers, where the representations are distinguished with respect to the order and the signs of the integers that are squared. Prove that $r_2(2n) = r_2(n)$, for any $n \in \mathbb{N}$.*

Solution: If $x^2 + y^2 = n$, then $(x + y)^2 + (x - y)^2 = 2n$. Conversely, if $s^2 + t^2 = 2n$, then s and t have the same parity and $\left(\frac{s+t}{2}\right)^2 + \left(\frac{s-t}{2}\right)^2 = n$. It is easy to check that $(x, y) \mapsto (x + y, x - y)$ is a bijection between the sets of representation of n and $2n$, respectively. ♢

Example 5.2. *Determine all integers that can be represented as a difference of squares of two integers.*

Solution: We claim that these are integers which are not of the form $4k + 2$.

Indeed, if $n \equiv 2 \pmod 4$ and $n = x^2 - y^2 = (x - y)(x + y)$, then one of the factors $x - y$, $x + y$ is even. But their difference $(x + y) - (x - y) = 2y$ is an even number, so both factors are even, which implies $n \equiv 0 \pmod 4$, a contradiction.

Conversely, if $n \not\equiv 2 \pmod 4$, then either $n = 2k + 1$ or $n = 4k$. In the first case, we have

$$2k + 1 = (k + 1)^2 - k^2,$$

and in the second case

$$4k = (k+1)^2 - (k-1)^2,$$

so, indeed, all integers which are not congruent to 2 modulo 4 can be represented as a difference of squares of two integers. ♢

Example 5.3. *Determine all positive integers which can be represented as a sum of squares of two positive integers.*

Solution: We claim that these are positive integers in whose prime factorization the exponent of any prime factor of the form $4k+3$ is even, and the exponent of the prime factor 2 is odd or there is at least one prime factor of the form 4k+1.

Necessity: Suppose that $n = 2^{2\alpha}m^2 = a^2 + b^2$, where all prime factors of m are of the form $4k+3$ and let n be the smallest positive integer with such property. If $\alpha > 0$, then a and b are even, so $2^{2(\alpha-1)}m^2 < n$ would have the same property. Hence, $\alpha = 0$ and $m^2 = a^2 + b^2$. However, m has a prime factor p of the form $4k+3$, so by Proposition 5.2, $p \mid a$ and $p \mid b$. Thus, $\left(\frac{m}{p}\right)^2 = \left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2$, which is a contradiction to the minimality of n.

Sufficiency: We have $n = 2m^2$ or $n = 2^\alpha m^2 l$, where $\alpha \in \{0,1\}$, and l is a product of prime factors of the form $4k+1$. If $n = 2m^2$, then $n = m^2 + m^2$.

Let $n = 2^\alpha m^2 l$. We claim that the number l is a sum of squares of two positive integers. Indeed, all its prime factors are such and the product of two odd numbers, which are sums of squares of two positive integers, is such, as well. Namely, if $p_1 = a^2 + b^2$, $p_2 = c^2 + d^2$, and if a and c, as well as b and d, have the same parity, then $p_1p_2 = (ad+bc)^2 + (ac-bd)^2$ and $ad+bc \neq 0$, $ac-bd \neq 0$ (because $ad+bc$ is positive and $ac-bd$ is odd). Now the claim follows by induction over the number of prime factors. Thus $l = s^2+t^2$, $s,t \in \mathbb{N}$, so $m^2l = (ms)^2+(mt)^2$ and $2m^2l = (ms+mt)^2+(ms-mt)^2$. Since l is odd, we conclude that $s \neq t$, so $ms - mt \neq 0$. ♢

Example 5.4. *If a positive integer n is not a sum of squares of two integers, then n is not a sum of squares of two rational numbers.*

Solution: If n is not a sum of squares of two integers, then n has a prime factor p of the form $4k+3$, which divides it to an odd power. Let us assume that $n = \left(\frac{a}{b}\right)^2 + \left(\frac{c}{d}\right)^2$. Then $n(bd)^2 = (ad)^2 + (bc)^2$. However, p divides the left-hand side of the equality to an odd power, so we obtained a contradiction to Theorem 5.7. ♢

Example 5.5. *Prove that the equation $x^2 - y^3 = 7$ has no integer solutions.*

Solution: For y even, we obtain $x^2 \equiv 7 \pmod 8$, which is impossible. For $y = 2k+1$, we have

$$x^2 + 1 = y^3 + 2^3 = (y+2)((y-1)^2 + 3).$$

The number $(y-1)^2 + 3 = 4k^2 + 3$ is $\equiv 3 \pmod 4$, so it has at least one prime factor p of the form $4n+3$. But such a prime number cannot divide $x^2 + 1^2$. ♢

The equation from Example 5.5 is a special case of the so-called Mordell's equation, and we will give more attention to it in Chapters 16.2 and 16.3.

Example 5.6. *Are the systems*

$$x^2 + 6y^2 = z^2, \quad 6x^2 + y^2 = t^2$$

and

$$x^2 + 7y^2 = z^2, \quad 7x^2 + y^2 = t^2$$

solvable in positive integers?

Solution: Without loss of generality, we can assume that x and y are relatively prime (otherwise, we divide the equations by a common factor). After adding one equation of the first system to the other, we obtain $7(x^2 + y^2) = z^2 + t^2$. From Proposition 5.2, it follows that $7 \mid z$ and $7 \mid t$. Hence, $7 \mid (x^2 + y^2)$, so after using the same argument as before, we conclude that $7 \mid x$ and $7 \mid y$, which is in a contradiction to the assumption that x and y are relatively prime. So, the first system has no solutions in positive integers.

The second system evidently has a solution $(x, y, z, t) = (3, 1, 4, 8)$. ♢

5.2 Positive definite binary quadratic forms

In this section, we will consider *binary quadratic forms*

$$f(x, y) = ax^2 + bxy + cy^2, \quad a, b, c \in \mathbb{Z},$$

i.e. homogeneous polynomials of degree 2 in two variables and integer coefficients, which is a generalization of the concepts from the previous section. The *discriminant* of f is $d = b^2 - 4ac$. Evidently, $d \equiv 0 \pmod 4$ if b is even and $d \equiv 1 \pmod 4$ if b is odd. The forms $x^2 - \frac{1}{4}dy^2$ if $d \equiv 0 \pmod 4$ and $x^2 + xy + \frac{1}{4}(1-d)y^2$ if $d \equiv 1 \pmod 4$ have the discriminant d and we call them the *principal forms* of discriminant d. For $d = -4$, we obtain the binary quadratic form $x^2 + y^2$ from the previous section.