5.3 Sums of four squares

In the previous sections, we have determined which numbers can be represented as a sum of two squares. We know that there are some numbers which cannot be represented in that form, for example, numbers 3 and 6. These two numbers can be represented as a sum of three squares, but the number 7 cannot be represented in that form. It is easily shown that number 7 can be represented as a sum of four squares ($7 = 2^2 + 1^2 + 1^2 + 1^2$). We might expect that now there is an exception again, a number that cannot be represented as a sum of four squares, but it can be represented as a sum of five squares. However, the following theorem, proved by the Italian-French mathematician Joseph-Louis Lagrange (1736 – 1813), demonstrates that there are no such exceptions and that every positive integer can be represented as a sum of four squares.

Theorem 5.14 (Four-square theorem (Lagrange)). *Every positive integer n can be represented as a sum of four squares, i.e. it can be written in the form $n = x^2 + y^2 + z^2 + w^2$, $x, y, z, w \in \mathbb{Z}$.*

Proof: Note that the following identity holds:

$$\begin{aligned}&(x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2)\\ &= (ax + by + cz + dw)^2 + (ay - bx + dz - cw)^2\\ &\quad + (az - cx + bw - dy)^2 + (aw - dx + cy - bz)^2. \end{aligned} \tag{5.3}$$

Therefore, it is sufficient to prove the statement of the theorem for prime numbers. It is clear that $2 = 1^2 + 1^2 + 0^2 + 0^2$, so let us assume that p is an odd prime number. Consider the numbers

$$0^2, 1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2 \tag{5.4}$$

that are pairwise incongruent modulo p (by Theorem 4.1). This also holds for the numbers

$$-1 - 0^2, -1 - 1^2, -1 - 2^2, \dots, -1 - \left(\frac{p-1}{2}\right)^2. \tag{5.5}$$

There are $p + 1$ numbers in (5.4) and (5.5) altogether. By Dirichlet's box principle, two of them have the same remainder modulo p. This means that there are integers x and y such that $x^2 \equiv -1-y^2 \pmod{p}$, i.e. $x^2+y^2+1 \equiv 0 \pmod{p}$, and $x^2 + y^2 + 1 < 1 + 2 \cdot (\frac{p}{2})^2 < p^2$. Thus, we conclude that $mp = x^2 + y^2 + 1 = x^2 + y^2 + 1^2 + 0^2$, for an integer $0 < m < p$.

Let l be the smallest positive integer such that $lp = x^2 + y^2 + z^2 + w^2$, for some $x, y, z, w \in \mathbb{Z}$. Then $l \leq m < p$. Furthermore, l is odd. Namely, if l were even, then we would have an even number (0, 2 or 4) of odd integers among x, y, z, w, and we could assume that $x + y$, $x - y$, $z + w$, $z - w$ are even. But, from

$$\frac{1}{2}lp = \Big(\frac{x+y}{2}\Big)^2 + \Big(\frac{x-y}{2}\Big)^2 + \Big(\frac{z+w}{2}\Big)^2 + \Big(\frac{z-w}{2}\Big)^2$$

we would obtain a contradiction with the minimality of l.

To prove the theorem, we have to show that $l = 1$. Hence, let us assume that $l > 1$ and try to obtain a contradiction.

Let x', y', z', w' be the absolutely least residues modulo p of x, y, z, w, respectively, and let

$$n = x'^2 + y'^2 + z'^2 + w'^2.$$

Then $n \equiv 0 \pmod{l}$ and $n > 0$ because otherwise, l would divide p. Furthermore, since l is odd, we have $n < 4 \cdot (\frac{l}{2})^2 = l^2$. Therefore, $n = kl$ for an integer k such that $0 < k < l$.

From identity (5.3), it follows that the number $(kl)(lp)$ can be represented as a sum of four squares, and moreover, any of those squares is divisible by l^2 ($xx' + yy' + zz' + ww' \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{l}$, $xy' - yx' + wz' - zw' \equiv xy - xy + zw - zw \equiv 0 \pmod{l}$ and analogously $xz' - zx' + +yw' - wy' \equiv 0 \pmod{l}$, $xw' - wx' + zy' - yz' \equiv 0 \pmod{l}$). Thus, the number kp can be represented as a sum of four squares, but this is in a contradiction with the minimality of l. $\square$

Legendre and Gauss proved that a positive integer n can be represented as a sum of three squares if and only if n is not of the form $4^m(8k + 7)$, $m, k \geq 0$. Necessity, which we will demonstrate in the following proposition, follows from the fact that squares are congruent to 0, 1 or 4 modulo 8. The proof of sufficiency, which is much more involved and uses the theory of ternary quadratic forms, will be presented in the next section.

Proposition 5.15. *Let $n = 4^m(8k + 7)$, $m, k \geq 0$. Then n cannot be written in the form $x^2 + y^2 + z^2$, $x, y, z \in \mathbb{Z}$.*

Solution: Suppose that the statement is not true and that n is the smallest positive integer for which the statement does not hold. Hence,

$$n = 4^m(8k + 7) = x^2 + y^2 + z^2.$$

The square of an odd number $(2a + 1)^2 = 8 \cdot \frac{a(a+1)}{2} + 1$ is congruent to 1 modulo 8. If among the numbers x, y, z there are 1, 2 or 3 odd numbers, then $x^2+y^2+z^2$ is of the form $4l+1$, $4l+2$ or $8l+3$, respectively. However, n does not have any of these forms. Hence, x, y, z are all even, so let $x = 2x_1$, $y = 2y_1$, $z = 2z_1$. Now, we have

$$\frac{n}{4} = 4^{m-1}(8k+7) = x_1^2 + y_1^2 + z_1^2,$$

so we obtained a contradiction with the minimality of n. $\diamondsuit$

Example 5.12. *Let us denote by $r_4(n)$ the number of representations of the number n as a sum of four squares, where we distinguish the representations with respect to the order of the summands and signs of the integers which are squared. Prove that $r_4(8n) = r_4(2n)$, for any $n \in \mathbb{N}$.*

Solution: If $8n = x_1^2 + x_2^2 + x_3^2 + x_4^2$, then all x_i are even. Indeed, if they are all odd, then $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 4 \pmod 8$, and if two of them are even and two odd, then $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 2 \pmod 4$. Therefore, $2n = \left(\frac{x_1}{2}\right)^2 + \left(\frac{x_2}{2}\right)^2 + \left(\frac{x_3}{2}\right)^2 + \left(\frac{x_4}{2}\right)^2$. Conversely, if $2n = y_1^2 + y_2^2 + y_3^2 + y_4^2$, then $8n = (2y_1)^2 + (2y_2)^2 + (2y_3)^2 + (2y_4)^2$. $\diamondsuit$

Example 5.13. *Prove that the number 2^{2k+1}, $k \in \mathbb{N}$ cannot be represented as a sum of squares of four positive integers.*

Solution: The only representation of number 2 as a sum of four squares is $2 = 1^2 + 1^2 + 0^2 + 0^2$ (by changing the order of the summands and the signs, we obtain exactly 24 different representations). Since $r_4(2^{2k+1}) = r_4(2^{2k-1}) = \cdots = r_4(2^1)$, the only representation of the number 2^{2k+1} as a sum of four squares is

$$2^{2k+1} = (2^k)^2 + (2^k)^2 + 0^2 + 0^2. \qquad \diamondsuit$$

If we distinguish the representations $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ according to the order of summands and signs of x_i's, then the number of representations $r_4(n)$ can be calculated by *Jacobi's formula*

$$r_4(n) = 8 \sum_{m|n,\ 4\nmid m} m$$

(for a proof see [211, Chapter 20]). In particular, $r_4(p) = 8(p+1)$ for a prime number p.

Example 5.14. *Prove that every integer $n > 169$ can be represented as a sum of squares of five positive integers.*

Solution: Let us write a positive integer $n-169$ as a sum of squares of four integers:

$$n-169=x_1^2+x_2^2+x_3^2+x_4^2, \quad x_1 \geq x_2 \geq x_3 \geq x_4 \geq 0.$$

If all $x_i>0$, then we write $169=13^2$. If $x_4=0$ and $x_3>0$, then we write $169=12^2+5^2$, so $n=x_1^2+x_2^2+x_3^2+12^2+5^2$. If $x_3=x_4=0$ and $x_2>0$, then we write $169=12^2+4^2+3^2$. Finally, if $x_2=x_3=x_4=0$, then we write $169=10^2+8^2+2^2+1^2$. ♢

Example 5.15. *Prove that every integer n can be written in the form $n = x^2+y^2-z^2$ in infinitely many ways.*

Solution: We distinguish two cases depending on whether n is odd or even (l is an arbitrary integer):

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

$$2k=(2l^2+2l-k)^2+(2l+1)^2-(2l^2+2l-k+1)^2. \qquad ♢$$

Example 5.16. *Prove that every positive integer n can be written in the form $x^2+2y^2+3z^2+6t^2$, where $x,y,z,t \in \mathbb{Z}$.*

Solution: We know that n can be written in the form $n=a^2+b^2+c^2+d^2$. We can assume that $a+b+c \equiv 0 \pmod 3$ (by changing the sign of one of the numbers a,b,c if necessary). This is clear if three numbers among a,b,c,d are divisible by 3. Otherwise, if, for example, a,b are not divisible by 3, then $a+b$ or $a-b$ is divisible by 3, so we take that $a+b$ is divisible by 3. If c is divisible by 3, then the number $a+b+c$ has the desired property, and if c is not divisible by 3, then one of the numbers $a-b+c$, $a-b-c$ has the desired property. We can additionally assume that $a \equiv b \pmod 2$ because two of the numbers a,b,c have the same parity. Let $a+b+c=3z$, $a+b=2k$, $a-b=2y$. Then we have

$$3(a^2+b^2+c^2)=(a+b+c)^2+2(k-c)^2+6y^2.$$

This implies that $3 \mid k-c$, i.e. $k-c=3t$, so we obtain

$$a^2+b^2+c^2=3z^2+6t^2+2y^2. \qquad ♢$$