Lagrange's four squares theorem

The purpose of this note is to prove the following result, due to the French mathematician *Joseph-Louis Lagrange* (1736-1813).

THEOREM. *Every nonnegative integer is the sum of four squares.*

The proof of the theorem consists of four main parts:

1. the multiplicative property,
2. the existence of solutions of $x^2 + y^2 + 1 = 0$ in $\mathbb{Z}_p$,
3. the descent argument,
4. the final inductive argument,

1 The multiplicative property

LEMMA 1. *Let x, y be integers each one of which is the sum of four squares of integers. Then the product $x.y$ is the sum of four squares of integers.*

PROOF. Let $x = a^2 + b^2 + c^2 + d^2$, $y = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$. Then, using the identity

$$\begin{aligned}(a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) \quad &= \quad (a\alpha - b\beta - c\gamma - d\delta)^2 \\ +(a\beta + b\alpha + c\delta - d\gamma)^2 + (a\gamma + c\alpha + d\beta - b\delta)^2 &+ (a\delta + d\alpha + b\gamma - c\beta)^2 \,,\end{aligned}$$

it follows that $x.y$ is the sum of four squares. $\diamondsuit$

REMARK. The indentity used in the proof of Lemma 1 may appear somewhat unnatural, the kind of formula that is easy to check once it has occurred to you to write it, but that you would never be able to discover on your own. That is not quite true. There is a simple way to discover this identity, by thinking about quaternions. (See the first set of notes.) $\diamondsuit$

2 Existence of solutions of $x^2 + y^2 + 1 = 0$ in $\mathbb{Z}_p$

LEMMA 2. *Let p be a prime. Then the equation $x^2 + y^2 + 1 = 0$ has a solution $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$. (That is, there exist members x, y of $\mathbb{Z}_p$ such that $x^2 + y^2 + 1 = 0$ in $\mathbb{Z}_p$.)*

The proof of Lemma 2 is left to you, as a homework problem (due on Dec. 16).

3 The descent argument

The basic idea of the descent argument is that, if n is a positive integer, and we can write a number of the form t^2n, for some positive integer t, as the sum of four squares, then if $t > 1$ we can "make t smaller," that is, we can "go down" and do the same thing for a number $\tau^2 n$, with τ a positive integer *smaller than* t. Once we know this, we can keep going down, until t becomes 1, that is, until we have expressed n itself as the sum of four squares.

The first step in the proof is to take care of factors of 2, by showing that if t is even, then we can go from t to $\frac{t}{2}$.

LEMMA 3. *Let n be an integer such that $2n$ is the sum of the squares of four integers. Then n is the sum of the squares of four integers.*

PROOF. Let a, b, c, d be integers such that

$$a^2 + b^2 + c^2 + d^2 = 2n\,.$$

Then either (a) a, b, c, d are odd, or (b) a, b, c, d are even, or (c) two of the numbers a, b, c, d are even and the other two are odd. In case (c), we can relabel a, b, c, d, if necessary, so that a and b are even and c and d are odd. Now, in all three cases, the numbers

$$\alpha = \frac{a+b}{2}\,, \quad \beta = \frac{a-b}{2}\,, \quad \gamma = \frac{c+d}{2}\,, \quad \delta = \frac{c-d}{2}$$

are integers. Furthermore,

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = n\,.$$

So n is the sum of four squares. $\diamondsuit$

LEMMA 4. *Let n, t be positive integers such that $t > 1$ and $t^2 n$ is the sum of four squares. Then there exists an integer τ such that $1 \le \tau < t$ with the property that $\tau^2 n$ is the sum of four squares.*

PROOF. If t is even, then we take $\tau = \frac{t}{2}$. Then $4\tau^2 n = t^2 n$. So $4\tau^2 n$ is the sum of four squares. Lemma 3, applied twice, implies that $\tau^2 n$ is the sum of four squares.

Now assume that t is odd. Let a, b, c, d be integers such that

$$a^2 + b^2 + c^2 + d^2 = t^2 n\,.$$

Let

$$\hat{a} = \frac{a}{t}\,, \qquad \hat{b} = \frac{b}{t}\,, \qquad \hat{c} = \frac{c}{t}\,, \qquad \hat{d} = \frac{d}{t}\,.$$

Then $\hat{a}$, $\hat{b}$, $\hat{c}$ and $\hat{d}$ are rational numbers and

$$\hat{a}^2 + \hat{b}^2 + \hat{c}^2 + \hat{d}^2 = n\,. \tag{1}$$

We now remark that $\hat{a}$ cannot be equal to $k + \frac{1}{2}$ for some integer k, because the equality $\frac{a}{t} = k + \frac{1}{2}$ would imply $2a = (2k+1)t$, which is impossible, since $2k+1$ and t are odd. Therefore there exists a unique integer $\tilde{a}$ closest to $\hat{a}$, and $\tilde{a}$ satisfies $|\hat{a} - \tilde{a}| < \frac{1}{2}$. Similarly, we let $\tilde{b}$, $\tilde{c}$, $\tilde{d}$, be the unique integers closest to $\hat{b}$, $\hat{c}$, $\hat{d}$, so $|\hat{b} - \tilde{b}| < \frac{1}{2}$, $|\hat{c} - \tilde{c}| < \frac{1}{2}$, $|\hat{d} - \tilde{d}| < \frac{1}{2}$. Let

$$\check{a} = \hat{a} - \tilde{a}\,, \qquad \check{b} = \hat{b} - \tilde{b}\,, \qquad \check{c} = \hat{c} - \tilde{c}\,, \qquad \check{d} = \hat{d} - \tilde{d}\,, \qquad \theta = \check{a}^2 + \check{b}^2 + \check{c}^2 + \check{d}^2\,.$$

Then $\check{a}$, $\check{b}$, $\check{c}$, $\check{d}$ are rational numbers, and $\theta < 1$. If $\theta = 0$, then $\hat{a}$, $\hat{b}$, $\hat{c}$ and $\hat{d}$ are integers, and (1) shows that we can satisfy our conclusion by taking $\tau = 1$.

Now let us assume that $0 < \theta < 1$. Let

$$\tau = \mu t{+}\nu\,, \qquad \alpha = \mu a{+}\nu\tilde{a}\,, \qquad \beta = \mu b{+}\nu\tilde{b}\,, \qquad \gamma = \mu c{+}\nu\tilde{c}\,, \qquad \delta = \mu d{+}\nu\tilde{d}\,,$$

where μ and ν are integers to be chosen later. Then

$$\begin{aligned}
\alpha^2 + \beta^2 + \gamma^2 + \delta^2 &= \mu^2(a^2 + b^2 + c^2 + d^2) + \nu^2(\tilde{a}^2 + \tilde{b}^2 + \tilde{c}^2 + \tilde{d}^2) \\
&\quad + 2\mu\nu(a\tilde{a} + b\tilde{b} + c\tilde{c} + d\tilde{d}^2) \\
&= \mu^2 t^2 n + \nu^2 n + 2\mu\nu t n + \nu^2(\tilde{a}^2 + \tilde{b}^2 + \tilde{c}^2 + \tilde{d}^2 - n) \\
&\quad + 2\mu\nu(a\tilde{a} + b\tilde{b} + c\tilde{c} + d\tilde{d}^2 - tn) \\
&= \tau^2 n + \nu A\,,
\end{aligned}$$

where

$$A = \nu(\tilde{a}^2 + \tilde{b}^2 + \tilde{c}^2 + \tilde{d}^2 - n) + 2\mu(a\tilde{a} + b\tilde{b} + c\tilde{c} + d\tilde{d}^2 - tn)\,.$$

Choose

$$\nu = -2(a\tilde{a} + b\tilde{b} + c\tilde{c} + d\tilde{d}^2 - tn)\,, \qquad \mu = \tilde{a}^2 + \tilde{b}^2 + \tilde{c}^2 + \tilde{d}^2 - n\,.$$

Then $A = 0$, so

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = \tau^2 n\,,$$

showing that $\tau^2 n$ is the sum of four squares. Furthermore,

$$\begin{aligned}
\tau &= \mu t + \nu \\
&= t(\tilde{a}^2 + \tilde{b}^2 + \tilde{c}^2 + \tilde{d}^2) - tn - 2(a\tilde{a} + b\tilde{b} + c\tilde{c} + d\tilde{d}^2 - tn) \\
&= t\Big(n + (\tilde{a}^2 + \tilde{b}^2 + \tilde{c}^2 + \tilde{d}^2) - 2(\hat{a}\tilde{a} + \hat{b}\tilde{b} + \hat{c}\tilde{c} + \hat{d}\tilde{d}^2)\Big) \\
&= t\Big((\hat{a}^2 + \hat{b}^2 + \hat{c}^2 + \hat{d}^2) + (\tilde{a}^2 + \tilde{b}^2 + \tilde{c}^2 + \tilde{d}^2) - 2(\hat{a}\tilde{a} + \hat{b}\tilde{b} + \hat{c}\tilde{c} + \hat{d}\tilde{d}^2)\Big) \\
&= t\Big((\hat{a} - \tilde{a})^2 + (\hat{b} - \tilde{b})^2 + (\hat{c} - \tilde{c})^2 + (\hat{d} - \tilde{d})^2\Big) \\
&= t(\check{a}^2 + \check{b}^2 + \check{c}^2 + \check{d}^2) \\
&= \theta t\,.
\end{aligned}$$

It follows that $0 < \tau < t$. So τ is a positive integer, $\tau < t$ and $\tau^2 n$ is the sum of four squares, and our proof is complete. ♢

LEMMA 5. *Let n, t be positive integers such that $t^2 n$ is the sum of four squares. Then n is the sum of four squares.*

PROOF. Since we are assuming that there exists a positive integer t such that $t^2 n$ is the sum of four squares, the well-ordering principle implies that there exists a smallest positive integer t such that $t^2 n$ is the sum of four squares. We will prove that $t = 1$.

Assume that $t > 1$. Then Lemma 4 implies that there exists a smaller positive integer τ such that $\tau^2 n$ is the sum of four squares, contradicting the fact that t is the smallest positive integer with that property. Therefore $t = 1$, and our proof is complete. ♢

4 The final inductive argument

We are now ready to conclude the proof of the four-squares theorem. We will do the proof using the well-ordering principle. Let $S(n)$ be the statement "n is a nonnegative integer and n cannot be expressed as the sum of four squares." We want to show that $S(n)$ is not true for any n. Suppose that $S(n)$ was true for some n. Then by the well-ordering principle there would exist a smallest n such that $S(n)$ is true. Call it p. (We are calling it p because, as we will soon see, this integer has to be prime.) Then p cannot be equal to 0, 1, or 2, because 0, 1 and 2 are sums of four squares, since $0 = 0^2+0^2+0^2+0^2$, $1 = 1^2+0^2+0^2+0^2$, and $2 = 1^2 + 1^2 + 0^2 + 0^2$. Therefore $p > 2$. Furthermore, p must be a prime number, because

1. if p is not prime then it is composite (since $p > 1$);

2. then we can write $p = a.b$, where a, b are positive integers such that $a < p$ and $b < p$;

3. then both a and b are sums of four squares, because p is supposed to be the smallest positive integer which is not a sum of four squares, and a, b are positive integers smaller than p;

4. then Lemma 1 implies that $a.b$ is the sum of four squares;

5. therefore p is the sum of four squares, contradiciting the fact that $S(p)$ is true.

Since p is prime and $p > 2$, p is an odd prime. Let $\nu = \frac{p-1}{2}$, so ν is an integer, since p is odd.

Using Lemma 2, we can pick $x, y \in \mathbb{Z}_p$ such that $x^2 + y^2 + 1 = 0$ in $\mathbb{Z}_p$. Therefore x and y are integers, $0 \le x < p$, $0 \le y < p$, and p divides x^2+y^2+1. Replacing x by $p-x$ does not change the fact that p divides $x^2 + y^2 + 1$, since $(p-x)^2 = (-x)^2 = x^2$ modulo p. So we may assume that $x \le \nu$, because if $x > \nu$ then $p - x < p - \nu = \nu + 1$, so $p - x \le \nu$. Similarly, we may assume that $y \le \nu$. We have therefore proved the existence if integers x, y, t such that $0 \le x \le \nu$, $0 \le y \le \nu$, and $x^2 + y^2 + 1 = t.p$. Since $x \le \nu$ and $y \le \nu$, we have

$$t.p = x^2 + y^2 + 1 \le 2\nu^2 + 1 \le 2\Big(\frac{p-1}{2}\Big)^2 + 1 = \frac{(p-1)^2}{2} + 1\,,$$

so

$$t \le \frac{p-1}{2} \cdot \frac{p-1}{p} + \frac{1}{p} < \frac{p-1}{2} + \frac{1}{2} = \frac{p}{2}\,,$$

so $t < \frac{p}{2}$ and then $t \le \nu$. In particular, $t < p$, so t is the sum of four squares. Since $t.p = x^2 + y^2 + 1 = x^2 + y^2 + 1^2 + 0^2$, the integer $t.p$ is the sum of four squares as well. Therefore Lemma 1 implies that the product $t^2p = t.(t.p)$ is the sum of four squares.

Then Lemma 6 implies that p itself is the sum of four squares. Therefore the statement $S(p)$ is false, and we have reached a contradiction. $\diamondsuit$