In this note we present proofs of the classical theorems concerning sums of two, three or four squares of integers. The main tool is Minkowki's convex body theorem. For the three squares theorem we follow Ankeny's 1957 paper [1]. In this case the proof also involves Dirchlet's theorem on primes in arithmetic progressions.

Theorem. *(Euler 1749) An integer $n \geq 1$ is a sum of two squares if and only every prime $q \equiv 3 \pmod 4$ divides n exactly an even number of times.*

Proof. Let p be a prime. Since -1 is not a square modulo p if and only if $p \equiv 3 \pmod 4$ and since the norm map $\mathbf{Z}[i] \longrightarrow \mathbf{Z}$ is multiplicative, it suffices to show that every prime $p \equiv 1 \pmod 4$ is a sum of two squares. Let a be an integer for which $a^2 \equiv -1 \pmod p$. The lattice

$$L = \{(x,y) \in \mathbf{Z}^2 : y \equiv ax \pmod p\}$$

has covolume p in $\mathbf{R}^2$. Every vector $(x,y) \in L$ satisfies $x^2+y^2 \equiv x^2+a^2x^2 \equiv 0 \pmod p$. The disk D of radius $\sqrt{2p}$ has area $2\pi p$. Since this exceeds 2^2p, Minkowski's convex body Theorem implies that there is a non-zero vector (x,y) in $L \cap D$. Therefore $x^2+y^2 < 2p$. Since $x^2+y^2 \equiv 0 \pmod p$ it follows that $x^2+y^2 = p$ as required.

Theorem. *(Lagrange 1770) Every integer $n \geq 1$ is a sum of 4 squares.*

Proof. Since the norm map from the ring of integral quaternions to $\mathbf{Z}$ is multiplicative and since $2 = 1^2+1^2+0^2+0^2$, it suffices to show that every prime $p > 2$ is a sum of four squares. Let p be a prime. Since the subsets of $\mathbf{Z}/p\mathbf{Z}$ given by

$$\{-a^2 : a \in \mathbf{Z}/p\mathbf{Z}\}, \qquad \text{and} \qquad \{b^2+1 : b \in \mathbf{Z}/p\mathbf{Z}\}$$

both have $(p+1)/2$ elements, their intersection is not empty. So, there do exist $a, b \in \mathbf{Z}$ for which $-a^2 \equiv b^2+1 \pmod p$. The lattice

$$L = \{(x,y,z,w) \in \mathbf{Z}^4 : z = ax+by \pmod p \text{ and } w = bx-ay \pmod p\}$$

has covolume p^2 in $\mathbf{R}^4$. Every vector (x,y,z,w) in L satisfies

$$x^2+y^2+z^2+w^2 \equiv x^2+y^2+(ax+by)^2+(bx-ay)^2 \equiv (a^2+b^2+1)(x^2+y^2) \equiv 0 \pmod p.$$

The ball B of radius $\sqrt{2p}$ in $\mathbf{R}^4$ has volume $\frac{\pi^2}{2}(\sqrt{2p})^4$. Since this exceeds 2^4p^2, Minkowski's Theorem implies that there is a non-zero vector (x,y,z,w) in $L \cap B$. This means that the expression $x^2+y^2+z^2+w^2$ is congruent to $0 \pmod p$ as well as $< 2p$. It follows that $x^2+y^2+z^2+w^2 = p$ as required.

Theorem. *(Legendre 1798; Gauss 1801) An integer $n \geq 1$ is the sum of three squares if and only if it is not of the form 4^km for some integer $m \equiv 7 \pmod 8$.*

Proof. A sum of three squares is never congruent to $7 \pmod 8$ and it is divisible by 4 if and only if each of the squares is. Therefore it suffices to show that every squarefree integer $m \not\equiv 7 \pmod 8$ is a sum of three squares. First we deal with the case $m \not\equiv 3 \pmod 8$. By

Dirichlet's theorem on primes in arithmetic progressions, there exists a prime number q satisfying

$$q \equiv -1 \pmod{m}, \qquad\qquad q \equiv \begin{cases} 1 \pmod{4}, & \text{when } m \equiv 1, 5 \pmod{8}; \\ 1 \pmod{8}, & \text{when } m \equiv 2 \pmod{8}; \\ 5 \pmod{8}, & \text{when } m \equiv 6 \pmod{8}. \end{cases}$$

Using quadratic reciprocity one checks that in each case the Legendre symbol $\left(\frac{-m}{q}\right)$ is $+1$, so that $-m$ is a square modulo q. Therefore there exists $b \in \mathbf{Z}$ satisfying $b^2 \equiv -m \pmod{q}$. The lattice

$$L \;=\; \{(x, y, z) \in \mathbf{Z}^3 : x \equiv y \pmod{m} \text{ and } y \equiv bz \pmod{q}\}$$

has covolume mq in $\mathbf{R}^3$. Every vector $(x, y, z) \in L$ satisfies

$$\begin{aligned} qx^2 + y^2 + mz^2 &\equiv -x^2 + y^2 \equiv 0 \pmod{m}, \\ &\equiv (bz)^2 + mz^2 \equiv 0 \pmod{q}. \end{aligned}$$

The ellipsoid E in $\mathbf{R}^3$ given by $qX^2+Y^2+mZ^2 \leq 2mq$ has volume $\frac{4\pi}{3}(\sqrt{2qm})^3/\sqrt{qm}$. Since this exceeds 2^3qm, there is a non-zero vector (x, y, z) in $L \cap E$. This means $qx^2+y^2+mz^2 < 2qm$ as well as $qx^2 + y^2 + mz^2 \equiv 0 \pmod{qm}$. Therefore we must have

$$qx^2 + y^2 + mz^2 = qm.$$

Let now $p \neq 2, q$ be a prime that divides $y^2 + mz^2$ an *odd* number of times. Then $-m$ is a square modulo p and $x^2 \equiv m \pmod{p}$. If p does not divide m, this implies at once that -1 is a square modulo p and hence $p \equiv 1 \pmod{4}$. If p divides m, it divides x and y. Therefore we have $mz^2 \equiv qm \pmod{p^2}$. Since m is squarefree, this implies that q is a square mod p. Since $q \equiv -1$ mod m and hence mod p, we see that $p \equiv 1 \pmod{4}$.

Therefore every prime $p \neq 2, q$ dividing $y^2 + mz^2$ an *odd* number of times is congruent to $1 \pmod{4}$. Since $q \equiv 1 \pmod{4}$, the two squares theorem implies that $(y^2 + mz^2)/q$ is a sum of two squares. This proves the theorem when $m \not\equiv 3 \pmod{8}$.

Case $m \equiv 3 \pmod{8}$. We modify this argument slightly. This time the prime q should satisfy $q \equiv -\frac{1}{2} \pmod{m}$ and $q \equiv 1 \pmod{4}$. Then $-m$ is a square mod q and there exists $b \in \mathbf{Z}$ such that $b^2 \equiv -m \pmod{4q}$. The lattice is replaced by

$$L \;=\; \{(x, y, z) \in \mathbf{Z}^3 : x \equiv y \pmod{m} \text{ and } y \equiv bz \pmod{2q}\}.$$

It has covolume $2mq$ in $\mathbf{R}^3$. This time the relevant quadratic form is $2qX^2 + Y^2 + mZ^2$. Every vector $(x, y, z) \in L$ satisfies

$$\begin{aligned} 2qx^2 + y^2 + mz^2 &\equiv -x^2 + y^2 \equiv 0 \pmod{m}, \\ &\equiv (bz)^2 + mz^2 \equiv 0 \pmod{2q}. \end{aligned}$$

The ellipsoid E given by $2qX^2 + Y^2 + mZ^2 \leq 4mq$ has volume $\frac{4\pi}{3}(2\sqrt{qm})^3/\sqrt{2qm}$. Since this exceeds $2^3 2qm$, there is a non-zero vector (x, y, z) in $L \cap E$. This means that $2qx^2 + y^2 + mz^2$ is congruent to $0 \pmod{2qm}$ as well as $< 4qm$. Therefore we have

$$2qx^2 + y^2 + mz^2 = 2qm.$$

The proof of the fact that any prime $p > 2$ dividing $y^2 + mz^2$ an *odd* number of times, is necessarily congruent to $1 \pmod 4$, is the same. This proves the theorem in the case $m \equiv 3 \pmod 8$.

[1] N. C. Ankeny.: Sums of three squares, *Proceedings of the AMS* **8** (1957), 316–319.