Math 361

April 7, 2023

Two squares theorem

Theorem. Let $p \in \mathbb{Z}$ be a prime number, and suppose that $p = 1 \bmod 4$. Then

$$p = x^2 + y^2$$

for some $x, y \in \mathbb{Z}$.

Proof

Step 1. Pick $u \in \{1, \ldots, p-1\}$ such that $u^2 = -1 \bmod p$.

Proof

Step 1. Pick $u \in \{1, \ldots, p-1\}$ such that $u^2 = -1 \bmod p$. Why this is possible:

$$(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

with $n_1 \geq 1$, $n_1 | n_2 | \cdots | n_k$ and some $k \geq 0$.

Proof

Step 1. Pick $u \in \{1, \ldots, p-1\}$ such that $u^2 = -1 \bmod p$. Why this is possible:

$$(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

with $n_1 \geq 1$, $n_1 | n_2 | \cdots | n_k$ and some $k \geq 0$. We get $p-1$ solutions to $x^{n_k} - 1 \in \mathbb{F}_p[x]$.

Proof

Step 1. Pick $u \in \{1, \ldots, p-1\}$ such that $u^2 = -1 \bmod p$. Why this is possible:

$$(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

with $n_1 \geq 1$, $n_1 | n_2 | \cdots | n_k$ and some $k \geq 0$. We get $p-1$ solutions to $x^{n_k} - 1 \in \mathbb{F}_p[x]$. So $n_k \geq p-1$.

Proof

Step 1. Pick $u \in \{1, \ldots, p-1\}$ such that $u^2 = -1 \bmod p$. Why this is possible:

$$(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

with $n_1 \geq 1$, $n_1|n_2|\cdots|n_k$ and some $k \geq 0$. We get $p-1$ solutions to $x^{n_k} - 1 \in \mathbb{F}_p[x]$. So $n_k \geq p-1$. But $n_1 \cdots n_k = p-1$.

Proof

Step 1. Pick $u \in \{1, \ldots, p-1\}$ such that $u^2 = -1 \bmod p$. Why this is possible:

$$(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

with $n_1 \geq 1$, $n_1 | n_2 | \cdots | n_k$ and some $k \geq 0$. We get $p-1$ solutions to $x^{n_k} - 1 \in \mathbb{F}_p[x]$. So $n_k \geq p-1$. But $n_1 \cdots n_k = p-1$. Hence, $n_k \leq p-1$.

Proof

Step 1. Pick $u \in \{1, \ldots, p-1\}$ such that $u^2 = -1 \bmod p$. Why this is possible:

$$(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

with $n_1 \geq 1$, $n_1 | n_2 | \cdots | n_k$ and some $k \geq 0$. We get $p-1$ solutions to $x^{n_k} - 1 \in \mathbb{F}_p[x]$. So $n_k \geq p-1$. But $n_1 \cdots n_k = p-1$. Hence, $n_k \leq p-1$. So $k = 1$, and $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.

Proof

Step 1. Pick $u \in \{1, \ldots, p-1\}$ such that $u^2 = -1 \bmod p$. Why this is possible:

$$(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

with $n_1 \geq 1$, $n_1 | n_2 | \cdots | n_k$ and some $k \geq 0$. We get $p-1$ solutions to $x^{n_k} - 1 \in \mathbb{F}_p[x]$. So $n_k \geq p-1$. But $n_1 \cdots n_k = p-1$. Hence, $n_k \leq p-1$. So $k = 1$, and $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.

By assumption, $p = 1 + 4k$ for some k.

Proof

Step 1. Pick $u \in \{1, \ldots, p-1\}$ such that $u^2 = -1 \bmod p$. Why this is possible:

$$(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

with $n_1 \geq 1$, $n_1|n_2|\cdots|n_k$ and some $k \geq 0$. We get $p-1$ solutions to $x^{n_k} - 1 \in \mathbb{F}_p[x]$. So $n_k \geq p-1$. But $n_1 \cdots n_k = p-1$. Hence, $n_k \leq p-1$. So $k = 1$, and $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.

By assumption, $p = 1 + 4k$ for some k. Let v be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$, and define $u = v^k$.

Proof

Step 1. Pick $u \in \{1, \ldots, p-1\}$ such that $u^2 = -1 \bmod p$. Why this is possible:

$$(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

with $n_1 \geq 1$, $n_1|n_2|\cdots|n_k$ and some $k \geq 0$. We get $p-1$ solutions to $x^{n_k} - 1 \in \mathbb{F}_p[x]$. So $n_k \geq p-1$. But $n_1 \cdots n_k = p-1$. Hence, $n_k \leq p-1$. So $k = 1$, and $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.

By assumption, $p = 1 + 4k$ for some k. Let v be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$, and define $u = v^k$. It follows that $u^4 = v^{4k} = v^{p-1} = 1 \bmod p$, and $u^2 \neq 1 \bmod p$ (since v has order 4).

Proof

Step 1. Pick $u \in \{1, \ldots, p-1\}$ such that $u^2 = -1 \bmod p$. Why this is possible:

$$(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

with $n_1 \geq 1$, $n_1|n_2|\cdots|n_k$ and some $k \geq 0$. We get $p-1$ solutions to $x^{n_k} - 1 \in \mathbb{F}_p[x]$. So $n_k \geq p-1$. But $n_1 \cdots n_k = p-1$. Hence, $n_k \leq p-1$. So $k = 1$, and $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.

By assumption, $p = 1 + 4k$ for some k. Let v be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$, and define $u = v^k$. It follows that $u^4 = v^{4k} = v^{p-1} = 1 \bmod p$, and $u^2 \neq 1 \bmod p$ (since v has order 4). Since

$$u^4 - 1 = (u^2 - 1)(u^2 + 1) = 0 \bmod p,$$

it follows that $u^2 = -1 \bmod p$.

Proof

Step 2. Having fixed $u \in \{1, \ldots, p-1\}$ such that $u^2 = -1 \bmod p$, define

$$L = \mathrm{Span}_{\mathbb{Z}}\{(0, p), (1, u)\} \subset \mathbb{Z}^2 \subset \mathbb{R}^2$$

Proof

Step 2. Having fixed $u \in \{1, \ldots, p-1\}$ such that $u^2 = -1 \bmod p$, define

$$L = \mathrm{Span}_{\mathbb{Z}}\{(0, p), (1, u)\} \subset \mathbb{Z}^2 \subset \mathbb{R}^2$$

Then L is a rank 2 lattice in $\mathbb{R}^2$, and the area of a fundamental domain F for L is

$$\left| \begin{pmatrix} 0 & 1 \\ p & u \end{pmatrix} \right| = p.$$

Proof

Step 3. Let X be the unit disc of radius r centered at the origin in $\mathbb{R}^2$ where $r^2 = \frac{3}{2}p$.

Proof

Step 3. Let X be the unit disc of radius r centered at the origin in $\mathbb{R}^2$ where $r^2 = \frac{3}{2}p$. We have

$$\mathrm{vol}(X) = \pi r^2$$

Proof

Step 3. Let X be the unit disc of radius r centered at the origin in $\mathbb{R}^2$ where $r^2 = \frac{3}{2}p$. We have

$$\mathrm{vol}(X) = \pi r^2 = \frac{3}{2}\pi p$$

Proof

Step 3. Let X be the unit disc of radius r centered at the origin in $\mathbb{R}^2$ where $r^2 = \frac{3}{2}p$. We have

$$\operatorname{vol}(X) = \pi r^2 = \frac{3}{2}\pi p > 4p = 2^2 \operatorname{vol}(F).$$

Proof

Step 3. Let X be the unit disc of radius r centered at the origin in $\mathbb{R}^2$ where $r^2 = \frac{3}{2}p$. We have

$$\operatorname{vol}(X) = \pi r^2 = \frac{3}{2}\pi p > 4p = 2^2 \operatorname{vol}(F).$$

Minkowski: there exists a nonzero lattice point $(x, y) \in L \cap X$.

Proof

Step 3. Let X be the unit disc of radius r centered at the origin in $\mathbb{R}^2$ where $r^2 = \frac{3}{2}p$. We have

$$\mathrm{vol}(X) = \pi r^2 = \frac{3}{2}\pi p > 4p = 2^2 \,\mathrm{vol}(F).$$

Minkowski: there exists a nonzero lattice point $(x, y) \in L \cap X$.

$(x, y) \in X \Rightarrow x^2 + y^2 \leq r^2 = \frac{3}{2}p < 2p$.

Proof

Step 3. Let X be the unit disc of radius r centered at the origin in $\mathbb{R}^2$ where $r^2 = \frac{3}{2}p$. We have

$$\mathrm{vol}(X) = \pi r^2 = \frac{3}{2}\pi p > 4p = 2^2 \,\mathrm{vol}(F).$$

Minkowski: there exists a nonzero lattice point $(x, y) \in L \cap X$.

$(x, y) \in X \Rightarrow x^2 + y^2 \leq r^2 = \frac{3}{2}p < 2p$.

$(x, y) \in L \Rightarrow x^2 + y^2$ is divisible by p (check).

Proof

Step 3. Let X be the unit disc of radius r centered at the origin in $\mathbb{R}^2$ where $r^2 = \frac{3}{2}p$. We have

$$\operatorname{vol}(X) = \pi r^2 = \frac{3}{2}\pi p > 4p = 2^2 \operatorname{vol}(F).$$

Minkowski: there exists a nonzero lattice point $(x, y) \in L \cap X$.

$(x, y) \in X \Rightarrow x^2 + y^2 \leq r^2 = \frac{3}{2}p < 2p$.

$(x, y) \in L \Rightarrow x^2 + y^2$ is divisible by p (check).

So $x^2 + y^2 = kp$ for some $k \in \mathbb{Z}_{>0}$.

Proof

Step 3. Let X be the unit disc of radius r centered at the origin in $\mathbb{R}^2$ where $r^2 = \frac{3}{2}p$. We have

$$\mathrm{vol}(X) = \pi r^2 = \frac{3}{2}\pi p > 4p = 2^2 \,\mathrm{vol}(F).$$

Minkowski: there exists a nonzero lattice point $(x, y) \in L \cap X$.

$(x, y) \in X \Rightarrow x^2 + y^2 \leq r^2 = \frac{3}{2}p < 2p$.

$(x, y) \in L \Rightarrow x^2 + y^2$ is divisible by p (check).

So $x^2 + y^2 = kp$ for some $k \in \mathbb{Z}_{>0}$.

However, $x^2 + y^2 < 2p$.

Proof

Step 3. Let X be the unit disc of radius r centered at the origin in $\mathbb{R}^2$ where $r^2 = \frac{3}{2}p$. We have

$$\mathrm{vol}(X) = \pi r^2 = \frac{3}{2}\pi p > 4p = 2^2 \,\mathrm{vol}(F).$$

Minkowski: there exists a nonzero lattice point $(x, y) \in L \cap X$.

$(x, y) \in X \Rightarrow x^2 + y^2 \leq r^2 = \frac{3}{2}p < 2p$.

$(x, y) \in L \Rightarrow x^2 + y^2$ is divisible by p (check).

So $x^2 + y^2 = kp$ for some $k \in \mathbb{Z}_{>0}$.

However, $x^2 + y^2 < 2p$.

It follows that $x^2 + y^2 = p$. $\square$

Four squares theorem

Theorem. Every positive integer is the sum of four integer squares. In other words, if $n \in \mathbb{Z}$, then there exist $a, b, c, d \in \mathbb{Z}$ such that

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

Proof

Step 1. It suffices to prove the result for primes p since

$$(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) =$$

Proof

Step 1. It suffices to prove the result for primes p since

$$(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2) =$$
$$(aA-bB-cC-dD)^2+(aB+bA+cD-dC)^2$$
$$+(aC-bD+cA+dB)^2+(aD+bC-cB+dA)^2$$

for all $a, b, c, d, A, B, C, D \in \mathbb{Z}$.

Proof

Step 2. The result holds for $p = 2$

Proof

Step 2. The result holds for $p = 2$ since $2 = 1^2 + 1^2 + 0^2 + 0^2$.

Proof

Step 3. Let p be an odd prime. We claim there exist $u, v \in \mathbb{Z}$ such that

$$u^2 + v^2 = -1 \bmod p.$$

Proof

Step 3. Let p be an odd prime. We claim there exist $u, v \in \mathbb{Z}$ such that

$$u^2 + v^2 = -1 \bmod p.$$

Reason:

$|\{u^2 \bmod p : u \in \{0, 1, \ldots, p-1\}\}| =$

Proof

Step 3. Let p be an odd prime. We claim there exist $u, v \in \mathbb{Z}$ such that

$$u^2 + v^2 = -1 \bmod p.$$

Reason:

$|\{u^2 \bmod p : u \in \{0, 1, \ldots, p-1\}\}| = \frac{p+1}{2}$.

Proof

Step 3. Let p be an odd prime. We claim there exist $u, v \in \mathbb{Z}$ such that

$$u^2 + v^2 = -1 \bmod p.$$

Reason:

$|\{u^2 \bmod p : u \in \{0, 1, \ldots, p-1\}\}| = \frac{p+1}{2}$.

$|\{-1 - v^2 \bmod p : v \in \{0, 1, \ldots, p-1\}\}|$

Proof

Step 3. Let p be an odd prime. We claim there exist $u, v \in \mathbb{Z}$ such that

$$u^2 + v^2 = -1 \bmod p.$$

Reason:

$|\{u^2 \bmod p : u \in \{0, 1, \ldots, p-1\}\}| = \frac{p+1}{2}$.

$|\{-1 - v^2 \bmod p : v \in \{0, 1, \ldots, p-1\}\}| = \frac{p+1}{2}$.

Proof

Step 3. Let p be an odd prime. We claim there exist $u, v \in \mathbb{Z}$ such that

$$u^2 + v^2 = -1 \bmod p.$$

Reason:

$|\{u^2 \bmod p : u \in \{0, 1, \ldots, p-1\}\}| = \frac{p+1}{2}$.

$|\{-1 - v^2 \bmod p : v \in \{0, 1, \ldots, p-1\}\}| = \frac{p+1}{2}$.

The two sets above are not disjoint since

Proof

Step 3. Let p be an odd prime. We claim there exist $u, v \in \mathbb{Z}$ such that

$$u^2 + v^2 = -1 \bmod p.$$

Reason:

$|\{u^2 \bmod p : u \in \{0, 1, \ldots, p-1\}\}| = \frac{p+1}{2}$.

$|\{-1 - v^2 \bmod p : v \in \{0, 1, \ldots, p-1\}\}| = \frac{p+1}{2}$.

The two sets above are not disjoint since $\frac{p+1}{2} + \frac{p+1}{2} = p + 1 > p$.

Proof

Step 3. Let p be an odd prime. We claim there exist $u, v \in \mathbb{Z}$ such that

$$u^2 + v^2 = -1 \bmod p.$$

Reason:

$|\{u^2 \bmod p : u \in \{0, 1, \ldots, p-1\}\}| = \frac{p+1}{2}$.

$|\{-1 - v^2 \bmod p : v \in \{0, 1, \ldots, p-1\}\}| = \frac{p+1}{2}$.

The two sets above are not disjoint since $\frac{p+1}{2} + \frac{p+1}{2} = p + 1 > p$.

So there exist $u, v \in \mathbb{Z}$ such that $u^2 = -1 - v^2 \bmod p$.

Proof

Step 4.

$$L = \mathrm{colspan}_{\mathbb{Z}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ u & v & p & 0 \\ -v & u & 0 & p \end{pmatrix}.$$

Proof

Step 4.

$$L = \mathrm{colspan}_{\mathbb{Z}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ u & v & p & 0 \\ -v & u & 0 & p \end{pmatrix}.$$

$\mathrm{vol}(F) = |\mathbb{Z}^4/L| = p^2$ for a fundamental domain F.

Proof

Step 4.

$$L = \mathrm{colspan}_{\mathbb{Z}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ u & v & p & 0 \\ -v & u & 0 & p \end{pmatrix}.$$

$\mathrm{vol}(F) = |\mathbb{Z}^4/L| = p^2$ for a fundamental domain F.

Apply Minkowski with X being a ball of radius $r = \sqrt{1.9p}$.

Proof

Step 4.

$$L = \mathrm{colspan}_{\mathbb{Z}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ u & v & p & 0 \\ -v & u & 0 & p \end{pmatrix}.$$

$\mathrm{vol}(F) = |\mathbb{Z}^4/L| = p^2$ for a fundamental domain F.

Apply Minkowski with X being a ball of radius $r = \sqrt{1.9p}$.

$\mathrm{vol}(X) = \frac{\pi^2 r^4}{2}$

Proof

Step 4.

$$L = \mathrm{colspan}_{\mathbb{Z}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ u & v & p & 0 \\ -v & u & 0 & p \end{pmatrix}.$$

$\mathrm{vol}(F) = |\mathbb{Z}^4/L| = p^2$ for a fundamental domain F.

Apply Minkowski with X being a ball of radius $r = \sqrt{1.9p}$.

$\mathrm{vol}(X) = \frac{\pi^2 r^4}{2} = \frac{\pi^2 (1.9)^2}{2} p^2$

Proof

Step 4.

$$L = \mathrm{colspan}_{\mathbb{Z}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ u & v & p & 0 \\ -v & u & 0 & p \end{pmatrix}.$$

$\mathrm{vol}(F) = |\mathbb{Z}^4/L| = p^2$ for a fundamental domain F.

Apply Minkowski with X being a ball of radius $r = \sqrt{1.9p}$.

$\mathrm{vol}(X) = \frac{\pi^2 r^4}{2} = \frac{\pi^2 (1.9)^2}{2} p^2 > 2^4 p^2$

Proof

Step 4.

$$L = \mathrm{colspan}_{\mathbb{Z}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ u & v & p & 0 \\ -v & u & 0 & p \end{pmatrix}.$$

$\mathrm{vol}(F) = |\mathbb{Z}^4/L| = p^2$ for a fundamental domain F.

Apply Minkowski with X being a ball of radius $r = \sqrt{1.9p}$.

$\mathrm{vol}(X) = \frac{\pi^2 r^4}{2} = \frac{\pi^2 (1.9)^2}{2} p^2 > 2^4 p^2 = 2^4 \,\mathrm{vol}(F)$

Proof

Step 4.

$$L = \mathrm{colspan}_{\mathbb{Z}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ u & v & p & 0 \\ -v & u & 0 & p \end{pmatrix}.$$

$\mathrm{vol}(F) = |\mathbb{Z}^4/L| = p^2$ for a fundamental domain F.

Apply Minkowski with X being a ball of radius $r = \sqrt{1.9p}$.

$\mathrm{vol}(X) = \frac{\pi^2 r^4}{2} = \frac{\pi^2 (1.9)^2}{2} p^2 > 2^4 p^2 = 2^4 \,\mathrm{vol}(F)$

Minkowski: there exists a nonzero $\ell = (a, b, c, d) \in L \cap X$.

Proof

Step 4.

$$L = \mathrm{colspan}_{\mathbb{Z}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ u & v & p & 0 \\ -v & u & 0 & p \end{pmatrix}.$$

$\mathrm{vol}(F) = |\mathbb{Z}^4/L| = p^2$ for a fundamental domain F.

Apply Minkowski with X being a ball of radius $r = \sqrt{1.9p}$.

$\mathrm{vol}(X) = \frac{\pi^2 r^4}{2} = \frac{\pi^2 (1.9)^2}{2} p^2 > 2^4 p^2 = 2^4 \,\mathrm{vol}(F)$

Minkowski: there exists a nonzero $\ell = (a, b, c, d) \in L \cap X$.

$\ell \in X \Rightarrow a^2 + b^2 + c^2 + d^2 \leq r^2 = 1.9p < 2p.$

Proof

Step 4.

$$L = \mathrm{colspan}_{\mathbb{Z}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ u & v & p & 0 \\ -v & u & 0 & p \end{pmatrix}.$$

$\mathrm{vol}(F) = |\mathbb{Z}^4/L| = p^2$ for a fundamental domain F.

Apply Minkowski with X being a ball of radius $r = \sqrt{1.9p}$.

$\mathrm{vol}(X) = \frac{\pi^2 r^4}{2} = \frac{\pi^2 (1.9)^2}{2} p^2 > 2^4 p^2 = 2^4 \,\mathrm{vol}(F)$

Minkowski: there exists a nonzero $\ell = (a, b, c, d) \in L \cap X$.

$\ell \in X \Rightarrow a^2 + b^2 + c^2 + d^2 \leq r^2 = 1.9p < 2p.$

$\ell \in L \Rightarrow a^2 + b^2 + c^2 + d^2 = 0 \bmod p.$

Proof

Step 4.

$$L = \mathrm{colspan}_{\mathbb{Z}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ u & v & p & 0 \\ -v & u & 0 & p \end{pmatrix}.$$

$\mathrm{vol}(F) = |\mathbb{Z}^4/L| = p^2$ for a fundamental domain F.

Apply Minkowski with X being a ball of radius $r = \sqrt{1.9p}$.

$\mathrm{vol}(X) = \frac{\pi^2 r^4}{2} = \frac{\pi^2 (1.9)^2}{2} p^2 > 2^4 p^2 = 2^4 \,\mathrm{vol}(F)$

Minkowski: there exists a nonzero $\ell = (a, b, c, d) \in L \cap X$.

$\ell \in X \Rightarrow a^2 + b^2 + c^2 + d^2 \leq r^2 = 1.9p < 2p$.

$\ell \in L \Rightarrow a^2 + b^2 + c^2 + d^2 = 0 \bmod p$.

So $a^2 + b^2 + c^2 + d^2 = kp$ is a positive multiple of p that is less then $2p$. Therefore, $a^2 + b^2 + c^2 + d^2 = p$. □