Hensel's Lemma and The Hasse-Minkowski Principle

Fahad Hossaini

I'd like to thank my professor Ehsaan Hossain and my classmate Mustafa Motiwala for their time, hard work and having to put up with me.

1. Hensel's Lemma

1.1. Preliminaries

We start by mentioning the p-adic absolute value.

$|x|_p = p^{-v_{p(x)}}$, where $v_p(x)$ is the valuation of x at p, or, the exponent at p in the prime factorization (or some similar factorization of x if p is not prime). We'll denote $|x|_p$ as $|x|$.

This absolute value is a norm on $\mathbb{Q}$ when p is prime, so we can complete $\mathbb{Q}$ as a metric space with respect to this norm. Then, quotienting by the maximal ideal of Cauchy sequences that converge to 0 (as this completion has an algebraic structure) creates $\mathbb{Q}_p$, which is now a field and complete metric space.

We can extend the absolute value on $\mathbb{Q}$ to $\mathbb{Q}_p$ without any complications. We define $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x| \leq 1\}$, or, the closed unit ball of $\mathbb{Q}$.

These numbers do have a nice intuition. If we write a number in base-p, then we consider the rightmost digits the most important, rather than the left most. Thus, $|1_p| > |10_p|$.

We'll mention some weird topological properties of $\mathbb{Q}_p$:

1. The strong triangle inequality holds in $\mathbb{Q}_p$, meaning: $\forall x, y \in \mathbb{Q}_p, |x + y| \leq \max\{|x|, |y|\}$, which is inherited from the absolute value. The following properties follow directly from this.
2. All triangles are isoceles, meaning $|x|, |y|, |x + y|$ can't all be different.
3. Every ball in $\mathbb{Q}_p$ is closed and open.
4. Every ball is either disjoint or the same.
5. $\mathbb{Q}_p$ is totally disconnected, meaning only singletons are the only connected sets.

The point being, we really do have a different structure than we expect on $\mathbb{R}$. So, from here on, we'll analyze these differences.

Now, we can state Hensel's Lemma.

Hensel's Lemma: Given a polynomial $f(x) \in \mathbb{Z}[x]$, and a prime p, if there exists some $x_1 \in \mathbb{Z}/p\mathbb{Z}$:

1. $f(x_1) \equiv 0 \bmod p$
2. $f'(x_1) \not\equiv 0 \bmod p$

Then, for every value of $n \in \mathbb{N}$, we can find some $x_{n+1} \equiv x_n \bmod p^n$ where $f(x_{n+1}) \equiv 0 \bmod p^{n+1}$. In particular, $\lim_{n\to\infty} x_n$ is a root for $f(x)$ in $\mathbb{Z}_p$.

1.2. Applying Hensel's Lemma

Let's see what Hensel's Lemma is really telling us. Given a polynomial, it gives a condition to not only determine if a polynomial has a root in $\mathbb{Q}_p$, but by following the proof, construct that root to our desired accuracy. We can think of n as the number of digits of precision we want.

Let's look at an example: $x^2 - 2$ with $p = 7$. In $\mathbb{Q}$, there isn't a root. But what about $\mathbb{Z}_7$?

Clearly, $3^2 - 2 \equiv 0 \bmod 7$ and that $f'(x) = 2x \not\equiv 0 \bmod p$ for all $x \in \mathbb{Z}/7\mathbb{Z}$. So, we should be able to construct a root that's always equivalent to the ones before.

The root is as follows in base-7: $...66421216213_7$

Writing this in base-7 is convenient because saying that $x_{n+1} \equiv x_n \bmod p^n$ means that in base-p, you share the first n digits. A finite truncation of this root gives us a solution to $f(x_n) \equiv 0 \bmod p^n$. Take $n = 2$. Then, $x_2 = 13_7 = 10$. Indeed, $10^2 - 2 = 98 \equiv 0 \bmod 49$.

Now, how can we prove this? We'll have to use the Taylor Series Expansion of the derivative and the Newton-Raphson method.

1.3. Taylor Series Expansion

We have to first define the derivative.

Let $f(x) = a_0 + a_1 x + ... + a_n x^n$ be a polynomial with coefficients in a ring R.

Then, $f'(x) = a_1 + 2a_2 x + ... + n a_{n-1} x^{n-1}$ is its formal derivative.

Now, we can state the necessary theorem:

If $f(x)$ is a polynomial with coefficients in a field $\mathbb{F}$ with characteristic zero, then, $\forall x, h \in \mathbb{F}$, we have:

$$f(x+h) = f'(x) + f'(x)h + \frac{1}{2!}f''(x)h^2 + \frac{1}{3!}f'''(x)h^3 + \cdots$$

Proof

We'll proceed by induction on the degree of an arbitrary polynomial of form $F(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ with coefficients in $\mathbb{Z}$.

For $n = 0$: $F(x+h) = a_0$

For $n = 1$:

$$F(x+h) = a_1(x+h) + a_0 = a_1 x + a_0 + a_1 h = F(x) + F'(x)h \text{ as } F'(x) = a_1$$

For the inductive step, we'll let $F(x)$ be an $n+1$ degree polynomial, and let $G(x) = F(x) - a_{n+1}x^{n+1}$.

Note that $\frac{F^{(k)}(x)}{k!} = \frac{G^{(k)}(x)}{k!} + a_{n+1}\binom{n+1}{k}x^{n+1-k}$ as $\binom{n+1}{k} = \frac{(n+1)!}{k!}$ is precisely our coefficient pulled from the exponent after k many derivatives.

We have:

$$\begin{aligned}
F(x+h) &= a_{n+1}(x+h)^{n+1} + a_n(x+h)^n + a_{n-1}(x+h)^{n+1} + \cdots \\
&= a_{n+1}\sum_{i=0}\binom{n+1}{i}x^{n+1-i}h^i + G(x+h) \\
&= a_{n+1}\sum_{i=0}\binom{n+1}{i}x^{n+1-i}h^i + G(x) + G'(x)h + \frac{1}{2!}G''(x)h^2 + \cdots \\
&= a_{n+1}x^{n+1} + a_{n+1}x^n h + a_{n+1}\binom{n+1}{2}x^{n-1}h^2 + \cdots + G(x) + G'(x)h + \frac{1}{2!}G''(x)h^2 + \cdots \\
&= a_{n+1}x^{n+1} + G(x) + a_{n+1}x^n h + G'(x)h + a_{n+1}\binom{n+1}{2}x^{n-1}h^2 + \frac{1}{2!}G''(x)h^2 + \cdots \\
&= F(x) + h(a_{n+1}x^n + G'(x)) + h^2\left(a_{n+1}\binom{n+1}{2}x^{n-1} + \frac{1}{2!}G''(x)\right) + \cdots \\
&= F(x) + h(F'(x)) + \frac{1}{2!}h^2(F''(x)) + \cdots + \frac{1}{(n+1)!}F^{(n+1)}(x)h^{n+1}
\end{aligned}$$

as desired. ■

It really is a matter of collecting like terms.

1.4. Proof of Hensel's Lemma

It's remarkable that the proof of Hensel's Lemma is quite elementary. It only uses the Newton-Raphson method, a tool many students learn in calculus. But this method is designed for finding roots of polynomials, after all. The only difference is, we can guarantee convergence in $\mathbb{Q}_p$.

Now that the Taylor Series is well defined, we can prove Hensel's Lemma.

Proof

Let $f(x) \in \mathbb{Z}[x]$, and a prime p be given so that there exists some $x_1 \in \mathbb{Z}/p\mathbb{Z}$ so that:

1. $f(x_1) \equiv 0 \bmod p$
2. $f'(x_1) \not\equiv 0 \bmod p$

Then, for every value of $n \in \mathbb{N}$, we can find some $x_{n+1} \equiv x_n \bmod p^n$ where $f(x_{n+1}) \equiv 0 \bmod p^{n+1}$. In particular, $\lim_{n\to\infty} x_n$ is a root for $f(x)$ in $\mathbb{Z}_p$.

We'll proceed by induction, noting that the base case is given, so we can do the inductive step directly.

Assume that $f(x_n) \equiv 0 \bmod p^n$, so $f(x_n) = p^n a$. Then, applying the Taylor Series expansion with $h = bp^n$, we get:

$$\begin{aligned}
f(x_n + bp^n) &= f(x_n) + bp^n f'(x_n) + b^2 p^{2n} f'' \frac{x_n}{2} + \cdots \\
&\equiv f(x_n) + bp^n f'(x_n) \bmod p^{n+1} \\
&\equiv ap^n + bp^n f'(x_n) \bmod p^{n+1} \\
&\equiv a + bf'(x_n) \bmod p
\end{aligned}$$

Since a is given and $f'(x_n) \equiv f'(x_1) \not\equiv 0 \bmod p$, we can solve for b so that $a + bf'(x_n)$ is equivalent to 0. This ensures some solution exists to $f(x) \bmod p^{n+1}$. So, we set $x_{n+1} = x_n + bp^n$. Then, $x_{n+1} \equiv x_n \bmod p^n$.

Finally, $\lim_{n\to\infty} x_n$ is a root for $f(x)$ in $\mathbb{Z}_p$ because for every $\varepsilon > 0$, we can ensure $|f(x_N)| < \varepsilon$ for some $N \in \mathbb{N}$, and $|f(x_m)| < |f(x_N)|$ for $m > N$. ■

We need to use Hensel's Lemma to prove that squares in $\mathbb{Q}_p$ take the following form: $x = p^{2v_p(x)} \cdot x'$ with $x' \in \mathbb{Z}_p$. Or, the valuation at the prime p must be even. We'll omit this proof for brevity.

1.5. Roots of Unity

One application of Hensel's Lemma is studying polynomials of the form $x^m = 1$ in $\mathbb{Q}_p$ for any value of m. The values of x that satisfy this polynomial are called mth roots of unity. They help us understand the structure of our space. Let's determine our roots of unity and valid values of m.

Let $f(x) = x^p - 1$. We'll attempt to find solutions.

The multiplicative group mod p tells us that $x^m \equiv 1 \bmod p$ for all x in our group if and only if m is a multiple of the order of the group, $p - 1$. Thus, we have $x^m \equiv 1 \bmod p$ for all $x \not\equiv 0 \bmod p$ when $m = k(p-1)$. We'll let $m = p - 1$ as we want to find the smallest such m that yields non-zero solutions. So, we have $p - 1$ solutions.

Then, $f'(x) = (p-1)x^{p-2}$. Since $(p-1) \not\equiv 0 \bmod p$ and $x \not\equiv 0 \bmod p$, we have that the derivative is non-zero for $x \not\equiv 0 \bmod p$. So, we have deduced that there are precisely $p - 1$ many $p - 1$th roots of unity.

2. The Hasse Minkowski Principle

2.1. The Local-Global Principle

Once again, Hensel's Lemma tells us about the existence of a root with minimal effort in $\mathbb{Z}_p$; Do a simple computation and check a derivative. So, finding a solution to a polynomial in $\mathbb{Z}_p$ and by extension, $\mathbb{Q}_p$ is really easy.

Since $\mathbb{Q} \subset \mathbb{Q}_p$ and both of them share similar structures, such as being rings (and by extension, we can use ring theory to get information for either $\mathbb{Q}$ or $\mathbb{Q}_p$) or the absolute value behaving nicely on both, a very reasonable question to ask is: Does information in $\mathbb{Q}_p$ tell us anything about $\mathbb{Q}$? Does information in local spaces, such as $\mathbb{Q}_p$, give us information about the global space, such as $\mathbb{Q}$? This is the idea behind the Local-Global Principle.

One such example is looking at roots of polynomials. One direction is easy; If we have a root to a polynomial in $\mathbb{Q}$, we have one in $\mathbb{Q}_p$. But what about the other direction? We have a very nice principle to describe this.

The Hasse Minkowski Principle: Given a quadratic form in n variables in $\mathbb{Q}$, say $x_1^2 + x_2^2 + \cdots + x_n^2$, the polynomial has a non-zero solution in $\mathbb{Q}$ if and only if it has a non-zero solution in every $\mathbb{Q}_p$ and $\mathbb{R}$.

2.2. Quadratic Forms

We first need to analyze quadratic forms. In particular, a quadratic form is: $\sum_i \sum_j a_{ij} x_i x_j$ for some suitable i, j, a_{ij}. So, $2x_1x_2 - \frac{2}{3}x_2x_3$ is a quadratic form of 3 variables. But this isn't like the one in the Hasse Minkowski Principle. We have to do some linear algebra to convince ourselves that the Hasse Minkowski Principle is well defined.

Performing a change of basis allows us to ensure that one quadratic form, say q_1, has the same solutions as another form q_2. But first, we need to represent quadratic forms as matrices. We'll do so as follows:

Let $q = \sum_i \sum_j a_{ij} x_i x_j$. Then, we define A to be the unique symmetric matrix so that a_{ij} comes from A. Then, we say that two quadratic forms are related if and only if the matrices of those forms are similar.

If q_1 has a solution, then applying the correct change of basis transformation will give us a solution in q_2, and vice versa.

Let's look at an example, $x^2 - 2xy + y^2$. We should see that $(1, 1)$ is a non-zero solution to this quadratic form. The matrix associated with this form is: $A = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$. Then, we'll diagonalize this matrix to get the matrix: $B = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$, $q_B = 2x^2$. Since A is similar to B, we see that B has a non-zero solution: $(0, 1)$.

Now, recall that since any symmetric matrix is diagonalizable, we can turn any quadratic form into one of the suitable form, where each variable is a square.

2.3. The Proof for $n \leq 3$

We start by noting that the complete proof is outside of the scope of this paper. We'll only show the proof for $n \leq 3$.

Proof

For all cases, note that is f has a solution in $\mathbb{Q}$, it will definitely have one in $\mathbb{Q}_p$ as $\mathbb{Q} \subset \mathbb{Q}_p$ and $\mathbb{Q} \subset \mathbb{R}$. So, we'll only show the reverse direction, or, assume a solution in every $\mathbb{Q}_p$ and $\mathbb{R}$ and show a solution exists in $\mathbb{Q}$.

$n = 1$:

In this case, no squares have a non-zero solution by looking at $\mathbb{R}$.

$n = 2$:

We start by showing that we can consider $f(x, y) = x^2 + cy^2$ with $c \in \mathbb{Z}$ and this is sufficient.

Since we are finding roots, we can multiply by the lowest common denominator to ensure our coefficients are in $\mathbb{Z}$. So, $f(x, y) = bx^2 + ay^2$. Then, we can multiply by b to get: $f(x, y) = b^2x^2 + aby^2$.

Then, by noting that a non-zero solution indeed exists, choosing $x' = \frac{x}{b}$ where x is from our original solution, we can eliminate b^2 in $f(x, y)$, and renaming $c = a \cdot b$, we get: $f(x) = x^2 + cy^2$.

Now, begin by recalling that $f(x, y)$ must have a non-zero solution in $\mathbb{R}$. So, $f(x, y) = x^2 - cy^2$ and $c > 0$. Rearranging yields: $c = \left(\frac{x}{y}\right)^2$. Since this equality holds in every $\mathbb{Q}_p$, all valuations are even, so $c \in \mathbb{Q}$ and c is a square, say $c = d^2$. So, $f(x, y) = x^2 - d^2y^2$. This is solvable by choosing $x = d^2$ and $y = 1$.

$n = 3$:

We owe this proof to Legendre, and we'll follow his steps.

We can consider $f(x, y, z) = x^2 + ay^2 + bz^2$ where a, b are integers and squarefree using a similar process as in the $n = 2$ case by multiplying and removing squares. Furthermore, we can show that $\gcd(a, b) = 1$ by noting that if $\gcd(a, b) > 1 = d$ and a solution exists, then

$d \mid x^2 \Rightarrow d|x$. So, we could absorb this factor into x. If $a = 0$ or $b = 0$, we have the case where $n = 2$. So, now, induct on $|a + b|$ as $a, b \in \mathbb{Z}$, where for the rest of the question, this denotes the absolute value in $\mathbb{R}$.

For our base case, $a = \pm 1, b = \pm 1$. So, $f(x, y, z) = \pm x^2 \pm y^2 \pm z^2$ By solution in $\mathbb{R}$, we must have alternating signs somewhere. Without loss of generality, let $f(x, y, z) = x^2 - y^2 \pm z^2$. Then, $(1, 1, 0)$ is a non-zero solution.

For our inductive step, assume that $2 \leq |a + b| < n + 1$ yields a solution. We'll show that $|a + b| = n + 1$ also yields a solution. Without loss of generality, assume $|a| < |b|$.

We want to prove the existence of some t, b' so that the following equation holds: $bb' = t^2 - a$ with $b' \geq 2$. Then, we can argue that $g(x, y, z) = x^2 - ay^2 \pm b'z^2$ has a non-zero solution if and only if $f(x, y, z)$ has a non-zero solution. So, we can tackle this problem with three steps.

1. Show that such t, b' exist.
2. Show that $g(x, y, z)$ has a non-zero solution if and only if $f(x, y, z)$ has a non-zero solution.
3. Show that $|b'| < |b|$ and make b' squarefree by removing all squares, so that we can apply the induction hypothesis.

We'll start with step 1. Showing that $bb' = t^2 - a$ is the same as showing that a is a square mod b. Since b is squarefree, we can write $b = p_1 p_2 \cdots p_k$. Let p_i be arbitrary. We'll show that a is a square mod p_i. If $a \equiv 0 \bmod p_i$, we're done.

Otherwise, note that $x^2 - ay^2 \pm bz^2 \equiv 0 \bmod p_i$ as we assumed there is a non-zero solution in $\mathbb{Q}_{p_i}$. Additionally, we can assume that one of x, y, z are not equivalent to $0 \bmod p_i$. (No one seems to explain why we can do so except saying the inverse limit structure of $\mathbb{Z}_p$).

Since $p_i \mid b$, we have: $x^2 - ay^2 \equiv 0 \bmod p_i$.

If $x \equiv 0 \bmod p_i$, as $p_i \nmid a$, we must have that $y \equiv 0 \bmod p_i$. Thus, $p_i^2 \mid f(x, y, z)$, and by extension, $p_i^2 \mid bz^2$. Since b is squarefree, we must have that $z \equiv 0 \bmod p_i$. But this contradicts that one of x, y, z are not equivalent to $0 \bmod p_i$.

So, $x^2 - ay^2 \equiv 0 \bmod p_i$ for nonzero x, so a must be a square mod p_i. Then, by the Chinese Remainder Theorem, since a is a square mod p_i for all suitable i, it must also be a square mod b. So, we can write $a \equiv t^2 \bmod b$ for some $t < b$. But by definition, this means $b'b = t^2 - a$ for some b' as desired.

Now, we can proceed with step 2. We'll show $f(x, y, z)$ has a non-zero solution in $\mathbb{Q}$ if and only if $b = x^2 - ay^2$. This will allow us to show that $g(x, y, z)$ has a solution.

Assume $b = x^2 - ay^2$. Then, $f(x, y, \pm 1) = x^2 - ay^2 - x^2 + ay^2 = 0$.

Now, assume that there's a non-zero solution in $\mathbb{Q}$. So, $x^2 - ay^2 \pm bz^2 = 0$. Note that $x \neq 0$, or else we would get: $a = \pm b\left(\frac{y}{z}\right)^2$ which is a contradiction as a is squarefree. Thus, $x \neq 0$. Rearranging yields:

$$x^2 \pm ay^2 = \pm bz^2$$

$$\frac{x^2}{z^2} - a\frac{y^2}{z^2} = \pm b$$

$$\left(\frac{x}{z}\right)^2 - a\left(\frac{y}{z}\right)^2 = \pm b$$

Thus, choosing b so that $\pm b = b$, and setting $x = \left(\frac{x}{z}\right)$ and $y = \left(\frac{y}{z}\right)$ yields the result.

Since $bb' = t^2 - a$, we know that $x^2 - ay^2 \pm bb'z^2$ has a non-zero solution when $f(x, y, z)$ has a non-zero solution.

The reason for this weird construction is that bb' is a norm in the quadratic number field $\mathbb{Q}(\sqrt{a})$. Then, we can use the fact that since bb' is a norm, we get the following relationship:

b is a norm if and only if b' is a norm. Or, a non-zero solution for b exists if and only if a non-zero solution for b' exists.

Now, we can proceed to step 3. Recall that $b \geq 2$. We can choose t so that $|t| \leq |\frac{b}{2}|$ by choosing the residue that falls into the first half of $\mathbb{Z}/b\mathbb{Z}$. We have the following equation:

$$|b'| = |\frac{t^2 - a}{b}| \leq |\frac{t^2}{b}| + |\frac{a}{b}| \leq |\frac{b^2}{4}| \cdot |\frac{1}{b}| + 1 = |\frac{b}{4}| + 1 < |b|$$

Finally, we need to ensure that b' is squarefree by removing squares. So let $b'' = b' \cdot u$ so that b'' is squarefree and u contains all even powers of b'. Since $|b''| \leq |b'|$ and b' must have some prime in its factorization, we see that $|b''| \geq 2$. Applying the induction hypothesis on $h(x) = x^2 - ay^2 \pm b''z^2$ results in $g(x)$ having as a non-zero solution. Thus, $f(x)$ has a non-zero solution, as desired.

■

Look at [1] for a similar proof to the Hasse-Minkowski Principle.

Unfortunately, despite how nice this theorem is, the Local-Global Principle fails to hold for higher degree polynomials.

2.4. Solving Quadratic Forms for $n = 3$

For simplicity, we'll write out quadratic form as $ax^2 + by^2 + cz^2$, and try to determine when this has non-zero solutions for different non-zero values of $a, b, c \in \mathbb{Q}$. We can use Hensel's Lemma and some elementary number theory to deduce these values.

We'll only try to determine what solutions exist in $\mathbb{Q}_p$ when p is odd and doesn't divide any of a, b, c.

Note that we can let each of a, b, c be pairwise coprime in the numerator, or we could divide out by the greatest common factor. Then, we can apply the same trick as in the proof to simplify to the case that a, b, c are integers.

We'll follow Gouvêa in [2] and prove that there exists some x_0, y_0, z_0 all not divisible by p so that:

$$ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \bmod p$$

Proof

By letting x, y, z range over all possible values, we have the following equation by Fermat's Little Theorem:

$$(ax^2 + by^2 + cz^2)^{p-1} \equiv \begin{cases} 1 \text{ if } (x, y, z) \text{ is not a solution} \\ 0 \text{ if } (x, y, z) \text{ is a solution} \end{cases}$$

Let $N \equiv \sum_{(x,y,z)} (ax^2 + by^2 + cz^2)^{p-1}$. Expanding this out, we see that any inner term must be written as $mx^{2i}y^{2j}z^{2k}$ by choosing i many x^2, j many y^2 and k many z^2 in the trinomial expansion, with $m \in \mathbb{Z}$. Thus, $2i + 2j + 2k = 2(p - 1)$. But notice that:

$$\begin{aligned} N &\equiv \sum_{(x,y,z)} \left[a^{p-1}x^{2(p-1)} + a^p b x^{2(p-2)} y^2 + a^{p-1} b^2 x^{2(p-3)} y^{2(2)} + \dots + c^{p-1} z^{2(p-1)}\right] \bmod p \\ &\equiv \sum_{(x,y,z)} a^{p-1}x^{2(p-1)} + \sum_{(x,y,z)} a^p b x^{2(p-2)} y^2 + \dots + \sum_{(x,y,z)} c^{p-1} z^{2(p-1)} \bmod p \end{aligned}$$

We want to show that $N \equiv 0 \bmod p$ since the triplet $(0,0,0)$ is a solution. Thus, if N is equivalent to 0, then, the number of non-zero solutions is $N - 1 \not\equiv 0 \bmod p$, and a non-zero solution exists.

So, all we need to show is that any combination of i, j, k results in the sum being 0.

Note that $\sum_{n=0}^{p-1} n^l \equiv 0 \bmod p$ for all $l < (p-1)$. To see this, note that there are less than $p - 1$ solutions of the polynomial $f(n) = 1 - n^l$. Letting m be a non-solution, we see that the sets $\{1, 2, ..., n-1\}$ and $\{m, 2m, ..., (n-1)m\}$ are in bijection. So, $\sum_{n=0}^{p-1} n^l = \sum_{n=0}^{p-1} (m \cdot n)^l$. Rearranging yields: $\left(1 - m^l\right) \sum_{n=0}^{p-1} n^l = 0$. As $\left(1 - m^l\right) \neq 0$ by construction, the sum is 0.

Notice that $2i + 2j + 2k = 2(p-1) \implies$ one of $2i, 2j, 2k < (p-1)$. Without loss of generality, let $2i < (p-1)$.

Now, consider the sum $\sum_{(x,y,z)} m x^{2i} y^{2j} z^{2k}$. We can rearrange to get:

$$\begin{aligned} \sum_{(x,y,z)} m x^{2i} y^{2j} z^{2k} &\equiv \sum_{(y,z)} \left[m y^{2j} z^{2k} \sum_{x=0}^{p-1} x^{2i} \right] \bmod p \\ &\equiv \sum_{(y,z)} m y^{2j} z^{2k} \cdot 0 \bmod p \\ &\equiv 0 \bmod p \end{aligned}$$

So, $N \equiv 0 \bmod p$ and by the existence of a trivial solution, the number of non-zero solutions is: $N - 1 \not\equiv 0 \bmod p$. ■

So, we know there exists some solution (x_0, y_0, z_0) to the quadratic form: $a x_0^2 + b y_0^2 + c z_0^2$. Then, turning this into a function with respect to x, we get: $f(x) = a x^2 + b y_0^2 + c z_0^2$.

Now, we can apply Hensel's Lemma. Choosing $x = x_0$ leads to a non-zero solution $\bmod p$.

Then, $f'(x) = 2ax \not\equiv 0$ as $a \neq 0$.

So, the only assumption we made is that p doesn't divide a, b, c or, p doesn't divide abc.

By this criteria, we see that $3x^2 \pm 5y^2 \pm 7z^2$ has a solution in $\mathbb{Q}_p$ for every $p > 7$. Indeed, choosing $f(x) = 3x^2 + 5y^2 - 7z^2$, we see that $(1, 2, 2)$ is a solution.

We list out the final list of criteria to see whether a quadratic form has a non-zero solution in $\mathbb{Q}$ by using the Hasse-Minkowski Principle, which can be found in [2]:

1. All of a, b, c don't share the same sign
2. For each odd prime dividing a, there exists some $r \in \mathbb{Z}$ so that $b + r^2 c \equiv 0 \bmod p$, and similarly for the odd primes dividing b and c.
3. If all of a, b, c are odd, then 4 divides one of: $a + b, a + c, b + c$.
4. If a is even, then 8 divides either $b + c$ or $a + b + c$, and similarly if b or c are even.

Bibliography

[1] J. Hatley, “Hasse-Minkowski and the Local-to-Global Principle.” [Online]. Available: https://www.math.union.edu/~hatleyj/Capstone.pdf

[2] F. Q. Gouvêa, *P-adic numbers: An introduction*. 2020.