ON THE EMBEDDING OF TRIANGLES
INTO INTEGER LATTICES

by

JAMES D. BLAIR

(Under the direction of Akos Magyar)

ABSTRACT

An important question in Number Theory has been ‘When can a positive integer \( l \) be written as the sum of \( n \) squares?’ This question has been answered and refined by Gauss and Jacobi, amongst many others. To generalize, consider the geometric version: ‘Are there vectors of length \( \sqrt{l} \) in \( \mathbb{Z}^n \)’? Then it is clear that there is a natural progression from embedding vectors, to triangles and higher dimensional simplices.

We start by analyzing what must be true if a triangle is realizable in \( \mathbb{Z}^n \). This yields some simple requirements; however the difficulty lies in finding sufficient conditions. Computational evidence suggests a 2-adic condition in 4 dimensions, while the necessary conditions are sufficient for \( n > 5 \).

Studying \( n = 4 \) for a local-global principle requires solving a system of equations \( p \)-adically for all primes. This is possible for \( p > 2 \); furthermore, a solution when \( p = 2 \) may be used to generate a global solution via the ring of Integer Quaternions. From there it follows that every admissible triangle sits in \( \mathbb{Z}^5 \).

The next natural problem is to estimate how many ways a triangle may be embedded. When \( n = 4 \), this uses a result of Siegel’s that a number \( l \) may be written as the sum of three squares in \( C_l t^{3-\epsilon} \) ways. For \( n = 5 \), methods of projecting down a dimension are computed, and then Siegel is applied again. A more analytic approach is then taken, generalizing the Circle Method. This amounts to considering rational scalings of the triangle, and provides an averaged version of the estimate.

Future development is suggested in two ways. First, higher dimensional simplices are more difficult to embed since many of the tools for triangles depend on the Quaternions. Analysis is still possible for odd primes \( p \), suggesting a 2-adic restriction again. Finally, by combining results with estimates for Fourier coefficients of modular forms (work being performed by others), a higher dimensional analogue of the equidistribution of points on spheres is possible.

INDEX WORDS: Simplices, Quaternions, Circle method, Equidistribution
ON THE EMBEDDING OF TRIANGLES
INTO INTEGER LATTICES

by

JAMES D. BLAIR

B.S., The University of South Carolina, 1997
B.S. in C.S., The University of South Carolina, 1997
M.S., The University of South Carolina, 1998

A Dissertation Submitted to the Graduate Faculty
of The University of Georgia in Partial Fulfillment
of the
Requirements for the Degree

DOCTOR OF PHILOSOPHY

ATHENS, GEORGIA

2004
ON THE EMBEDDING OF TRIANGLES
INTO INTEGER LATTICES

by

JAMES D. BLAIR

Approved:

Major Professor: Akos Magyar

Committee: Robert Rumely
Matthew Baker
Robert Varley
Edward Azoff

Electronic Version Approved:

Maureen Grasso
Dean of the Graduate School
The University of Georgia
August 2004
Acknowledgements

I would like to thank my wife Paula for all her love and patience over the last few months and years, as we worked through the challenges of making career and school go together. My appreciation also extends to our families who have been very supportive of us and my staying in school for so long.

Also, I could not have accomplished this without the advice of Dr. Magyar and Dr. Rumely over the years.
# Table of Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ACKNOWLEDGEMENTS</strong></td>
<td>iv</td>
</tr>
<tr>
<td><strong>1 BACKGROUN</strong></td>
<td>1</td>
</tr>
<tr>
<td><strong>2 FUNDAMENTAL RESULTS</strong></td>
<td>5</td>
</tr>
<tr>
<td>2.1 <strong>NECESSARY CONDITIONS</strong></td>
<td>5</td>
</tr>
<tr>
<td>2.2 <strong>USEFUL FACTS</strong></td>
<td>6</td>
</tr>
<tr>
<td>2.3 <strong>EMBEDDING IN 12 DIMENSIONS</strong></td>
<td>8</td>
</tr>
<tr>
<td><strong>3 CHARACTERIZATION OF TRIANGLES IN</strong> $\mathbb{Z}^4$</td>
<td>11</td>
</tr>
<tr>
<td>3.1 <strong>P-ADIC SOLUTIONS FOR ODD PRIMES</strong> $p$</td>
<td>11</td>
</tr>
<tr>
<td>3.2 <strong>P-ADIC SOLUTIONS FOR</strong> $p = 2$</td>
<td>14</td>
</tr>
<tr>
<td>3.3 <strong>QUATERNIONS</strong></td>
<td>17</td>
</tr>
<tr>
<td>3.4 <strong>EMBEDDABILITY IN</strong> $\mathbb{Z}^4$</td>
<td>21</td>
</tr>
<tr>
<td><strong>4 CHARACTERIZATION OF TRIANGLES IN</strong> $\mathbb{Z}^5$</td>
<td>23</td>
</tr>
<tr>
<td>4.1 <strong>EMBEDDING INTO</strong> $\mathbb{Z}^5$</td>
<td>23</td>
</tr>
<tr>
<td>4.2 <strong>NUMBER OF EMBDIE</strong></td>
<td>29</td>
</tr>
<tr>
<td><strong>5 ANALYTIC METHODS</strong></td>
<td>33</td>
</tr>
<tr>
<td>5.1 <strong>FOUNDATIONS</strong></td>
<td>33</td>
</tr>
<tr>
<td>5.2 <strong>MATRIX ESTIMATES</strong></td>
<td>34</td>
</tr>
<tr>
<td>5.3 <strong>MINOR ARCS</strong></td>
<td>41</td>
</tr>
</tbody>
</table>
A fundamental problem in Number Theory is to find solutions of Diophantine equations, that is polynomial equations with integer coefficients. One of the simplest questions to state of this sort is ‘When may a positive integer \( l \) be written as the sum of \( n \) squares?’ Lagrange, Gauss, Jacobi and many others contributed to solving this problem along with its derivatives. For example, a number may be written as the sum of two squares if every prime congruent to three in its factorization appears an even number of times (Fermat). A number may be written as the sum of three squares if and only if it is not of the form \( 4^t(8k-1) \) (Gauss). And every integer may be written as the sum of four squares (Lagrange). Jacobi’s primary contribution was an expression for the number of different ways a number may be written as the sum of four squares; in the process he set many of the foundations for analytical methods.

The question may be translated into geometric terms, where it becomes ‘When is there a vector in \( \mathbb{Z}^n \) with length \( \sqrt{l} \)?’ This in turn amounts to finding lattice points on spheres of a given radius. An intriguing question then arises when the radius of such a sphere is scaled up by a factor \( \lambda \), and the new lattice points are projected back onto the original sphere. As the scaling constant \( \lambda \) increases, more points of this type are located on the sphere, and it can be shown that they become equidistributed. That is, averaging a continuous function \( \phi \) over these points is equivalent, in the limit, to integrating it over the sphere, or

\[
\lim_{\lambda \to \infty} \frac{1}{N_{n,\lambda}} \sum_{m \in \mathbb{Z}^n, |m|^2 = k} \Phi \left( \frac{m}{\sqrt{\lambda}} \right) = \int_{S^{n-1}} \Phi(x) d\sigma
\]
Here $N_{n,\lambda}$ is the number of lattice points on the sphere $S^{n-1}$ of radius $\sqrt{\lambda}$. This result has been known for $n \geq 5$, but has only relatively recently been extended down as far as $n \geq 3$ using difficult estimates for Fourier coefficients of modular forms.

Since vectors may be considered to be one dimensional simplices, a natural generalization of this problem is to find representations for triangles in lattices $\mathbb{Z}^n$. In particular, assume the triangle with sides $\alpha, \beta, \gamma$ is under consideration; taking one vertex to be at the origin, the question becomes finding vectors $\mathbf{X}$ and $\mathbf{Y} \in \mathbb{Z}^n$ satisfying $|\mathbf{X}|^2 = \alpha^2, |\mathbf{Y}|^2 = \beta^2$ and $|\mathbf{X} - \mathbf{Y}|^2 = \gamma^2$. Taking $a = \alpha^2, b = \beta^2, c = \gamma^2$ and $e = (a + b - c)/2$, it is easy to show that these numbers must all be integers and must satisfy the inequality $|e| < \sqrt{ab}$. A triangle meeting these criteria will be called admissible.

The first major result will be a classification of those admissible triangles in four and five dimensions which are also embeddable. A surprisingly simple result that $ab - e^2$ be the sum of three squares is necessary and sufficient when $n = 4$. Also, when $n = 5$, every admissible triangle will be embeddable. The proofs of these facts are based on the algebraic structure of $\mathbb{Z}^4$, taking advantage of properties from the ring of integral quaternions.

The next result, akin to Jacobi’s work in the one dimensional case, is to estimate the number of representations of these triangles in the respective dimensions. The key principle here is Siegel’s result that a number $l$ which is writable as the sum of three squares may be expressed as such a sum in at least $C_* l^{1/2-\epsilon}$ different ways. In four dimensions, this implies that an embeddable triangle with $\Delta = ab - e^2$ may be realized in $C_* \Delta^{1/2-\epsilon}$ different ways. Continuing this process to five dimensions requires a more careful argument; as on spheres, scaling up by a factor of 4 does not generate more lattice points. Hence the corresponding result is that for a given triangle $T$,
there are asymptotically $C \lambda^{2-\epsilon}$ embeddings of the scaled triangle $\lambda T$, where $\lambda$ is odd.

Then there is a generalization of the last estimate to higher dimensions $n$. The problem is rephrased in an averaged form, counting the number of similar triangles in a lattice whose component vectors have bounded box norms. That is, for a given admissible triple $(a, b, e)$, $X$ and $Y$ satisfy $\max(x_i, 1 \leq i \leq n) \leq P$, $\max(y_i, 1 \leq i \leq n) \leq P$, $|X|^2 = \lambda a$, $|Y|^2 = \lambda b$ and $XY = \lambda e$, where $\lambda \in \mathbb{Q}$ and $\lambda a, \lambda b, \lambda e \in \mathbb{Z}$.

Define $N_P$ to be the number of solution vectors $X$ and $Y$ to this problem. Then by applying the Hardy-Littlewood method of exponential sums, $N_P$ can be computed as $P^{2n-4} \rho \prod_p A_p + E_P(a, b, e)$, where $E_P$ is an error term bounded by $CP^{2n-4-\frac{1}{6}}$. Here, $\rho$ will be the measure of a certain surface, hence positive, and $A_p$ is the density of $p$-adic solutions, which will also be positive.

A natural extension of these problems is to higher dimensional simplices; however, since the proof for triangles depends heavily on the Integer Quaternions, the methods given do not generalize well. A local-global principle has run throughout the work thus far, and one hopes that it can be extended. With that thought, the computations involved in showing that there are local solutions to the $k$-simplex problem for $n \geq 2k + 1$ are carried out for all odd primes.

The final direction taken here is to a generalization of the equidistribution result listed for spheres. Define $M(a, b, e)$ to be the set of all points $(X, Y)$ in $\mathbb{R}^{2n}$ which give an embedding of the triangle associated to the admissible triple $(a, b, e)$. Since any triangle in $\mathbb{R}^n$ may be rotated to any other congruent triangle, there is a natural action of $SO(n)$ on $M$. Furthermore, any rotation which fixes a triangle also must fix the plane that triangle lies in. Therefore, $M$ is a compact, smooth manifold which realizes the space $SO(n)/SO(n - 2)$.

Now, as in the result for spheres, fix $(a, b, e)$ and define $M_\lambda$ to be $M(\lambda a, \lambda b, \lambda e)$. Then as $\lambda$ grows, new lattice points are found which may be projected back to the
original surface $M$. Then the equidistribution of these points is expressed by the corresponding equation

$$
\lim_{\lambda \to \infty, \text{odd}} \frac{1}{N_\lambda} \sum_{X, Y \in M_\lambda \cap \mathbb{Z}^{2n}} \Phi \left( \frac{X}{\sqrt{\lambda}}, \frac{Y}{\sqrt{\lambda}} \right) = \int_M \Phi(x, y) d\sigma(x, y)
$$

where $\Phi$ is a smooth function and $N_\lambda$ is the number of lattice points on $M_\lambda$. Proving this result requires a lower bound on $N_\lambda$, which is provided by this dissertation. However it also requires some very difficult estimates on the Fourier coefficients of certain modular forms, in order to provide an upper bound for the summation term; this work is currently being carried out by Arpad Toth.
To begin, the focus shall be on determining exactly when a triangle with sides of lengths $\alpha$, $\beta$ and $\gamma$ can be embedded into the integer lattice $\mathbb{Z}^n$.

2.1 Necessary Conditions

The first question to answer is ‘What must be true about $\alpha$, $\beta$ and $\gamma$ given that they are associated to an embedded triangle?’ Consider $X = (x_1, x_2, \ldots, x_n)$ with $|X| = \alpha$ and $Y = (y_1, y_2, \ldots, y_n)$ with $|Y| = \beta$. Then $|X|^2 = x_1^2 + x_2^2 + \cdots + x_n^2 = \alpha^2$. Since all of the $x_i$ are to be integers, it is clear that $\alpha^2$, and correspondingly $\beta^2$, must be integers.

Furthermore, since $|X - Y| = \gamma$, it also follows that $|X - Y|^2 = |X|^2 - 2XY + |Y|^2 = \alpha^2 - 2\beta^2 = \gamma^2$ is an integer. Thus, $XY = x_1y_1 + \cdots + x_ny_n = (\alpha^2 + \beta^2 - \gamma^2)/2$ is an integer. By the triangle inequality, $\gamma > |\alpha - \beta|$, so $|(\alpha^2 + \beta^2 - \gamma^2)/2| < |(\alpha^2 + \beta^2 - \alpha^2 + 2\alpha\beta - \beta^2)/2| = \alpha\beta$.

**Theorem 2.1** If $\alpha$, $\beta$ and $\gamma$ are the lengths of the sides of a triangle which may be embedded into $\mathbb{Z}^n$ for some $n$, then the triangle may be characterized by the triple $(a, b, e)$ where $a = \alpha^2$, $b = \beta^2$ and $e = (\alpha^2 + \beta^2 - \gamma^2)/2$ are all integers. In order to be an actual triangle, the conditions $a > 0$, $b > 0$ and $|e| < \sqrt{ab}$ must also hold.

The next question is, ‘Are these necessary conditions sufficient?’ For $n < 4$ they clearly are not, since $a$ could be 7, which can not be written as the sum of any fewer than four squares. Thus, the triangle with side lengths $\sqrt{7}$, $\sqrt{7}$ and $\sqrt{6}$ can not be
embedded in $\mathbb{Z}^n$ for $n < 4$. [Note that the triangle with sides of length $\sqrt{7}, \sqrt{7}$ and $\sqrt{7}$ can never be embedded in any $\mathbb{Z}^n$ since then $e$ would not be an integer].

Thus, the goal is to determine if these conditions are ever sufficient, and if so, for which dimensions $n$. In particular, the system of equations

$$
\begin{align*}
x_1^2 + x_2^2 + \cdots + x_n^2 &= a \\
y_1^2 + y_2^2 + \cdots + y_n^2 &= b \\
x_1y_1 + \cdots + x_ny_n &= e
\end{align*}
$$

(2.1)

will be studied. It shall generally be assumed that $e \geq 0$, since if $e < 0$, then $x_i$ may be replaced by $-x_i$, leaving $a$ and $b$ unchanged while negating the value of $e$.

2.2 Useful Facts

Several fundamental facts shall be used throughout this paper, hence are presented here. The first two are well established theorems on writing integers as the sums of squares.

**Theorem 2.2 (Gauss)** A positive integer $m$ may be written as the sum of three squares if and only if $m$ is not of the form $4^l(8k-1)$ for $k, l$ integral.

**Theorem 2.3 (Lagrange)** Any positive integer $m$ may be written as the sum of four squares.

A useful technique for simplifying some of the ensuing problems involves replacing a given triangle with another one in such a way that either both triangles are embeddable in a given lattice, or neither is. The method chosen is presented in the following lemma.

**Lemma 2.4** If the triangle with vertices $< A, B, C >$ is characterized by the triple $(a, b, e)$, then the triangle $< A + (A - B), B + (A - B), C >$ is characterized by
(4a − 4e + b, a, 2a − e). In particular, the latter triangle is embeddable in a lattice if and only if the former one is. Finally, introducing the discriminant \( \Delta = ab - e^2 \), note that this transformation leaves \( \Delta \) unchanged.

**Proof:** The transformation effectively replaces the side of the triangle between \( A \) and \( B \) with a new side from \( 2A - B \) to \( A \). If \( A \) and \( B \) are integral lattice points, it follows immediately that \( 2A - B \) is as well; similarly, if \( A \) and \( 2A - B \) are integral lattice points, then so is \( B \). This proves that either both or neither of the triangles are embeddable in a given lattice.

The change from the characterization \((a, b, e)\) to \((4a - 4e + b, a, 2a - e)\) follows from noting that \(|2A - B|^2 = 4|A|^2 - 4|A \cdot B| + |B|^2 = 4a - 4e + b\), and similarly \(|(2A - B) \cdot A| = 2a - e\).

From there, it can be directly computed that \( \Delta \) remains fixed. Alternatively, observe that \( \Delta \) can be interpreted as four times the square of the area of the triangle; since the area is unchanged by this action, neither is \( \Delta \). QED

Finally, many computations will use a scaling property present when \( n = 4 \). The result follows from a matrix computation, hence may be applied to any value of \( n \) which is a multiple of four, although that corollary will not be used here.

**Lemma 2.5** If \( n = 4 \) and the triangle characterized by \((a, b, e)\) is embeddable into \( \mathbb{Z}^4 \), then for all positive integers \( k \), the triangle characterized by \((ka, kb, ke)\) is also embeddable into \( \mathbb{Z}^4 \).

**Proof:** Using Lagrange’s theorem, write \( k \) as \( k_1^2 + k_2^2 + k_3^2 + k_4^2 \), and consider the following matrix \( M_k \):

\[
\begin{bmatrix}
k_1 & k_2 & k_3 & k_4 \\
k_2 & -k_1 & k_4 & -k_3 \\
k_3 & -k_4 & -k_1 & k_2 \\
k_4 & k_3 & -k_2 & -k_1
\end{bmatrix}
\]
Then $M_k$ gives a transformation of $\mathbb{Z}^4$ into itself. Consider it as a change of basis matrix; hence the column vectors are images of the standard basis vectors in $\mathbb{Z}^4$. These column vectors are all orthogonal to each other, and all have norm $k$. Thus, the transformation preserves angles, and scales vectors by a factor of $\sqrt{k}$.

Therefore, $M_k$ maps a triangle $<0, X, Y>$ characterized by $(a, b, e)$ to a triangle $<0, M_kX, M_kY>$ characterized by $(ka, kb, e')$. Finally, since $e' = (a' + b' - c')/2 = (ka + kb - kc)/2 = ke$, the desired result follows. QED

The fact that such an $M_k$ exists is a direct consequence of the existence of the Quaternion group. In fact, the quaternions will play an even more important role in the analysis of triangles in $\mathbb{Z}^4$.

2.3 Embedding in 12 dimensions

Define a triple $(a, b, e)$ to be admissible if all of the necessary conditions for embeddability are met; that is, $a, b$ and $e$ are all integers where $a$ and $b$ are positive and $|e| < \sqrt{ab}$.

By taking $n = 12$, it can be shown that satisfying admissability is sufficient to guarantee an embedding. The proof proceeds by considering right, acute and obtuse triangles separately. Note that if a triangle can be embedded in $n$ dimensions, then it can clearly be embedded in $n + 1$ dimensions.

Lemma 2.6 If $n \geq 8$, then any right triangle characterized by the triple $(a, b, e)$ may be embedded into $\mathbb{Z}^n$.

Proof: Suppose $X$ and $Y$ are the legs of a right triangle represented by $(a, b, e)$, with as usual that $|X| = a$ and $|Y| = b$. Then since $X$ is perpendicular to $Y$, it follows that $e = X \cdot Y = 0$. By Lagrange’s theorem, $a$ can be written as $a_1^2 + a_2^2 + a_3^2 + a_4^2$ and $b$ as $b_1^2 + b_2^2 + b_3^2 + b_4^2$, where the $a_i$ and $b_i$ are all integers. Then take $X$ to be $(a_1, a_2, a_3, a_4, 0, 0, 0, 0)$ and $Y$ to be $(0, 0, 0, 0, b_1, b_2, b_3, b_4)$. QED
Proceeding to the acute case uses the law of cosines to show that $e$ must be smaller than both $a$ and $b$; from there it is trivial to obtain an embedding.

**Lemma 2.7** If $n \geq 12$, then any acute triangle characterized by the triple $(a, b, e)$ may be embedded into $\mathbb{Z}^n$.

**Proof:** Assume that the sides of the triangle have been ordered so that $a \geq b \geq c$. By the law of cosines (keeping in mind that $a$, $b$ and $c$ are the squares of the lengths of the sides of the triangle), $a = b + c - 2 \sqrt{bc} \cos \theta$, where $\theta$ is the measure of the angle opposite the side of length $\sqrt{a}$. In particular, this angle is acute, hence $\cos \theta > 0$ and thus $a < b + c$. Now this implies that $e = (a + b - c)/2 < ((b + c) + b - c)/2 = b$.

Therefore, $b - e > 0$ and $a - e > 0$. Let $e = e_1^2 + \cdots + e_4^2$, $b - e = \beta_1^2 + \cdots + \beta_4^2$ and $a - e = \alpha_1^2 + \cdots + \alpha_4^2$. Then take $X = (e_1, e_2, e_3, e_4, \alpha_1, \alpha_2, \alpha_3, \alpha_4, 0, 0, 0, 0)$ and $Y = (e_1, e_2, e_3, e_4, 0, 0, 0, 0, \beta_1, \beta_2, \beta_3, \beta_4)$. QED

Finally, the method of descent is applied to the obtuse triangles, via a series of reductions using Lemma 2.4, which must eventually terminate in either a right or acute triangle. Since the process always shortens the length of the longest side of the triangle, the descent must be completed in a finite number of steps.

**Theorem 2.8** If $n \geq 12$, then any admissible triple $(a, b, e)$ gives a triangle which is embeddable into $\mathbb{Z}^n$.

**Proof:** By Lemmas 2.6 and 2.7, only obtuse triangles remain to be considered.

Let $A$, $B$ and $C$ be the vertices of the triangle, and suppose that the angle at $C$ is acute. Consider the points $A + k(A - B)$, where $k$ is an integer, as well as $L$, the line which goes through these points. Then there is a point $Q$ on $L$ such that $QC$ is perpendicular to $L$. Note that since the triangle is obtuse, $A$ and $B$ lie on the same side of the line from $Q$. There are two possibilities to consider.
Case 1: There exists a choice for $k$ such that $A + k(A - B) = Q$. Let $A' = Q$ and $B' = A + (k - 1)(A - B)$. Then $< A', B', C >$ is a right triangle. By repeated application of Lemma 2.4, $< A', B', C >$ is characterized by some $(a', b', 0)$, hence is embeddable. Therefore the original triangle is embeddable.

Case 2: There exists a choice for $k$ such that $A + k(A - B)$ and $A + (k - 1)(A - B)$ lie on opposite sides of $Q$. Call these points $A'$ and $B'$ respectively. Now, if the triangle $< A', B', C >$ is acute, apply Lemmas 2.4 and 2.7 and the proof is done. Otherwise, assume without loss of generality that $CB$ is the longest side of the original triangle.

Next, $A'$ and $B'$ lie on $L$ between the points $B$ and $2Q - B$. Since $A$ was on the same side of $Q$ as $B$ was, it is impossible for $A$ to be $2Q - B$. Therefore the strict inequalities $|CA'| < |CB|$ and $|CB'| < |CB|$ hold. And trivially, $|A'B'| = |AB| < |CB|$. Therefore, the longest side of the new obtuse triangle is strictly shorter than the longest side of the original triangle. Since the new triangle was obtained from the original one by a series of $k$ applications of Lemma 2.4, it is characterizeable by an admissible triple $(a', b', e')$. Therefore the length of its longest side must also be the square root of an integer, hence this descent can only continue for a finite number of steps. QED
Thus far, it has been shown that for any triangle to embeddable in $\mathbb{Z}^n$ for $n \geq 12$, it is necessary and sufficient for it to be characterized by an admissible triple $(a, b, e)$. However, while the methods of the last chapter provided interesting ways to consider these embeddings, they clearly were not sharp results. As such, the next goal is to determine the smallest $n$ for which the conditions are sufficient.

Evidence gathered using the computer program listed in the Appendix indicated that there is a strong 2-adic condition governing which admissible triples give triangles which are embeddable in four dimensions (as well as giving concrete examples of triangles that are not). Using Lemma 2.5 to reduce the problem, it becomes reasonable to determine what this 2-adic condition is, and to prove that a local-global principle is at work.

3.1 P-adic solutions for odd primes $p$

For this section, $p$ shall represent an odd prime. In order to reinforce the idea that embedding a triangle in four dimensions is entirely based on a 2-adic condition, it will first be shown that there are no obstructions to embeddability amongst the odd primes. In particular, a solution to the Equations 2.1 will be found with the $x_i$ and $y_i$ in $\mathbb{Z}_p$ (the $p$-adic integers) for any choice of $(a, b, e)$.

Consider the matrix $M_p$ as in Lemma 2.5; with it, a triangle represented by $(a, b, e)$ can easily be taken to a triangle represented by $(pa, pb, pe)$. Therefore, if
a solution over \( \mathbb{Z}_p \) can be found for all triples \((a, b, e)\) with \( p \nmid \text{gcd}(a, b, e) \), then solutions can be found for any valid triple.

By using a version of Hensel’s Lemma to lift solutions mod \( p \) to \( \mathbb{Z}_p \), the problem reduces even further to just finding linearly independent vectors \( \mathbf{X} \) and \( \mathbf{Y} \) which are defined up to congruence mod \( p \).

**Lemma 3.1** If there is a linearly independent solution to

\[
\begin{align*}
    x_1^2 + x_2^2 + x_3^2 + x_4^2 &\equiv a \pmod{p^k} \\
    y_1^2 + y_2^2 + y_3^2 + y_4^2 &\equiv b \pmod{p^k} \\
    x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 &\equiv e \pmod{p^k}
\end{align*}
\]

for \( k = 1 \) and \( k = l \), then a lift may be made to a solution of these equations mod \( p^{l+1} \). Therefore, by repeated application of this lemma, a solution among the \( p \)-adic integers may be found.

**Proof:** Since the new solution should reduce to the solution assumed to exist by hypothesis, it follows that \( x'_i = x_i + a_ip^l \) and \( y'_i = y_i + b_ip^l \) for some set of integers \( a_i \) and \( b_i \). Thus, the equations to be solved are

\[
\begin{align*}
    \sum_{i=1}^{4} (x_i + a_ip^l)^2 &\equiv a + \delta_ap^l \pmod{p^{l+1}} \\
    \sum_{i=1}^{4} (y_i + b_ip^l)^2 &\equiv b + \delta_bp^l \pmod{p^{l+1}} \\
    \sum_{i=1}^{4} (x_i + a_ip^l)(y_i + b_ip^l) &\equiv e + \delta_ep^l \pmod{p^{l+1}}
\end{align*}
\]

In turn, since \( p \neq 2 \), these reduce to finding \( a_i \) and \( b_i \) such that

\[
\begin{align*}
    \sum_{i=1}^{4} x_ia_i &\equiv 2^{-1}\delta_a \pmod{p} \\
    \sum_{i=1}^{4} y_ib_i &\equiv 2^{-1}\delta_b \pmod{p} \\
    \sum_{i=1}^{4} x_ib_i + y_ia_i &\equiv \delta_e \pmod{p}
\end{align*}
\]
Since the original equations are linearly independent, assume without loss of gener-
ality that \( x_1y_2 - x_2y_1 \not\equiv 0 \mod p \) and furthermore that \( x_1y_2 \not\equiv 0 \mod p \). There are
eight unknowns and only three equations, so simplify by assuming that \( a_2 = a_3 = a_4 = b_3 = b_4 = 0 \). Then the equations are equivalent to the matrix form
\[
\begin{bmatrix}
  x_1 & 0 & 0 \\
  0 & y_1 & y_2 \\
  y_1 & x_1 & x_2 
\end{bmatrix}
\begin{bmatrix}
  a_1 \\
  b_1 \\
  b_2 
\end{bmatrix}
\equiv
\begin{bmatrix}
  2^{-1}\delta_a \\
  2^{-1}\delta_b \\
  \delta_e 
\end{bmatrix}
\pmod{p}
\]

Now, the determinant of the matrix is \( x_1(x_2y_1 - x_1y_2) \) which is not congruent to 0 \( \mod p \) since neither factor is 0 \( \mod p \); thus the matrix is invertible over \( \mathbb{Z}_p \). Multiplying both sides of the matrix equation by this inverse then yields values for \( a_1, b_1 \) and \( b_2 \) which can be used to satisfy the congruence \( \pmod{p^l+1} \). QED

**Theorem 3.2** For \( n \geq 4 \) and \( p \) an odd prime, there is a solution to Equations 2.1 over the \( p \)-adic integers \( \mathbb{Z}_p \), for any choice of \((a, b, e)\).

**Proof:** Let \( n = 4 \); finding a solution to the equations for this \( n \) automatically provides solutions for all larger \( n \). Also, let \( k \) be the integer such that \( p^k \mid \gcd(a, b, e) \).
Redefine \( a \) as \( a/p^k \), \( b \) as \( b/p^k \) and \( e \) as \( e/p^k \). Any embedding \( X \) and \( Y \) which satisfies Equations 2.1 for the new values of \( a, b \) and \( e \) may be adapted to an embedding \( M_{p^k}X \) and \( M_{p^k}Y \) satisfying the Equations for the original values.

With this additional condition, if \( p \nmid a \) and \( p \nmid b \), then \( p \nmid e \). Since \( p \neq 2 \) it follows that \( p \nmid a + b - c \) and finally \( p \nmid c \). That is, \( p \nmid \gcd(a, b, c) \) implies that \( p \nmid \gcd(a, b, c) \), so without loss of generality, assume that \( p \nmid a \).

Note that any \( \alpha \) may be written as \( \alpha \equiv \alpha_1^2 + \alpha_2^2 + \alpha_3^2 \pmod{p} \) where the \( \alpha_i \) are not all 0 \( \pmod{p} \). Furthermore, if \( \alpha \not\equiv 0 \pmod{p} \), then \( \alpha \) can be written as \( \alpha \equiv \alpha_1^2 + \alpha_2^2 \pmod{p} \) where again the \( \alpha_i \) are not all 0 \( \pmod{p} \).

Since \( p \nmid a \), let \( a \equiv x_1^2 + x_2^2 \pmod{p} \), with \( x_1 \not\equiv 0 \). Proceed by cases on the values of \( e \) and \( b \):
Case 1: Suppose \( e \equiv b \equiv 0 \mod p \). Write \( b \) as \( b \equiv (-x_2)^2 + x_1^2 + y_3^2 + y_4^2 \mod p \) with \( y_3 \not\equiv 0 \), using the fact that \( b - (-x_2)^2 - x_1^2 \equiv -a \not\equiv 0 \mod p \). Then there are the linearly independent solutions \( X = [x_1, x_2, 0, 0] \) and \( Y = [-x_2, x_1, y_3, y_4] \).

Case 2: Suppose \( e \equiv 0 \mod p \) and \( b \not\equiv 0 \mod p \). Then write \( b \equiv y_3^2 + y_4^2 \mod p \), again with \( y_3 \not\equiv 0 \), and there are the linearly independent solutions \( X = [x_1, x_2, 0, 0] \) and \( Y = [0, 0, y_3, y_4] \).

Case 3: Suppose \( e \not\equiv 0 \mod p \) and \( b - (ex_1^{-1})^2 \equiv 0 \mod p \). If \( x_2 \not\equiv 0 \), there are the linearly independent solutions \( X = [x_1, x_2, 0, 0] \) and \( Y = [ex_1^{-1}, b_2, b_3, b_4] \) where \( b_2^2 + b_3^2 + b_4^2 \equiv 0 \) and \( b_2 \not\equiv 0 \).

Case 4: Suppose \( e \not\equiv 0 \mod p \) and \( b - (ex_1^{-1})^2 \not\equiv 0 \mod p \). Then \( b \equiv (ex_1^{-1})^2 + y_3^2 + y_4^2 \), with \( y_3 \not\equiv 0 \), and there are the linearly independent solutions \( X = [x_1, x_2, 0, 0] \) and \( Y = [ex_1^{-1}, 0, y_3, y_4] \).

Now, by Lemma 3.1, these independent vectors lift to solutions over \( \mathbb{Z}_p \). QED

3.2 \( p \)-adic solutions for \( p = 2 \)

Now consider the case \( p = 2 \), with the goal of proving that there is a local-global principle at work. That is, given an admissible triple \((a, b, e)\), it follows immediately that the associated triangle is embeddable in \( \mathbb{R}^2 \), and hence in \( \mathbb{R}^4 \). By Theorem 3.2, the triangle is also embeddable in \( \mathbb{Z}_p^4 \) for all odd primes \( p \). Therefore, all that remains to be shown is that being embeddable in \( \mathbb{Z}_p^4 \) is equivalent to being embeddable in \( \mathbb{Z}_2^4 \).

The forward direction is trivial, so suppose that for a given triple \((a, b, e)\), there is a solution to Equations 2.1 over \( \mathbb{Z}_2 \). The process will be to show that this implies \( ab - e^2 \) is the sum of three squares. This condition in turn shall have a corresponding statement among the integer quaternions, a ring in which a form of factorization may
be applied. Then this factorization will give the choices for $X$ and $Y$. The following theorems will be necessary.

**Theorem 3.3 (Hasse-Minkowski)** In order that a quadratic form $f$ over the rationals represent 0, it is necessary and sufficient that the form $f_v$ represent 0 for all places $v$ of $\mathbb{Q}$.

In particular, this theorem can be restated with any integer $m$ in place of 0. Then consider the quadratic form $x_1^2 + x_2^2 + x_3^2 = m$; Hasse-Minkowski implies that $m$ can be written as the sum of three rational squares if and only if it can be written as the sum of three real squares (taking $v$ to be the place at infinity) and as the sum of three $p$-adic squares for all primes $p$. If this occurs, then the following lemma, a specialization of a result by Davenport-Cassels, becomes applicable.

**Lemma 3.4** An integer $m$ which may be written as the sum of three rational squares may also be written as the sum of three integral squares.

**Proof:** Let $f(X) = x_1^2 + x_2^2 + x_3^2$ where $X = (x_1, x_2, x_3) \in \mathbb{Q}^3$. Suppose there is a choice for $X$ such that $f(X) = m$. Then by clearing denominators, it follows that $f(Y) = t^2m$ for some $Y \in \mathbb{Z}^3$. Choose $t_0$ to be the smallest positive integer such that $f(Y) = t_0^2m$ has such a solution. The lemma follows from proving that $t_0 = 1$.

Write $Y/t_0$ as $R + S$ where $R \in \mathbb{Z}^3$ and $S \in \mathbb{Q}^3$ with $\max(|s_1|, |s_2|, |s_3|) \leq \frac{1}{2}$. If $S = (0, 0, 0)$, then $Y/t_0$ has all integral coefficients and satisfies $f(Y/t_0) = m$. By the minimality of $t_0$, this means that $t_0 = 1$.

Otherwise, consider the following change of variables. Let $a = f(R) - m$ and $b = 2mt_0 - 2YR$. Then set $t' = at_0 + b$ and $Y' = aY + bR$. Now $f(Y') = Y'Y' = a^2Y^2 + 2abYR + b^2R^2 = a^2t_0^2m + ab(2mt_0 - b) + b^2(m + a)$. This expression simplifies as $m(a^2t_0^2 + 2abt_0 + b^2) = mt'^2$. Thus $t'$ was a possible choice for $t_0$, hence $|t'| \geq t_0$. 


However, \( t_0' = at_0^2 + bt_0 = (R^2 - m)t_0^2 + (2mt_0 - 2YR)t_0 = t_0^2R^2 - 2t_0YR + Y^2 \).

This last term is \( (t_0R - Y)^2 = (t_0S)^2 = t_0^2f(S) \), so \( t_0' = t_0f(S) \). However, by the choice of \( S \), it is clear that \( 0 < f(S) < 1 \), hence \( 0 < t_0' < t_0 \). This contradicts the minimality of \( t_0 \), so it must be the case that \( t_0 = 1 \). QED

With these results in mind, it is possible to take a 2-adic solution and obtain information amongst the integers.

**Lemma 3.5** If \( X, Y \in \mathbb{Z}_4^2 \) are vectors yielding a solution to Equations 2.1, then \( ab - e^2 \) can be written as the sum of three squares.

**Proof:** Abusing notation slightly, let \( M_a \) be the 4x4 matrix over \( \mathbb{Z}_2 \) with coefficients arranged as in \( M_k \) and first row equal to \( X \). Then \( M_a \) gives a transformation of \( \mathbb{Z}_4^2 \) into itself which scales vectors by a factor of \( \sqrt{a} \).

So \( |M_aY|^2 = e^2 + r_1^2 + r_2^2 + r_3^2 = ab \), where the \( r_i \in \mathbb{Z}_2 \). Then \( ab - e^2 \) is the sum of three 2-adic squares. Since Theorem 3.2 guarantees solutions to Equations 2.1 for all odd primes \( p \), a symmetric argument also guarantees that \( ab - e^2 \) can be written as the sum of three \( p \)-adic squares. Finally, since \( (a, b, e) \) is an admissible triple, \( ab - e^2 \) is positive, hence can trivially be written as the sum of three real squares. But then by Hasse-Minkowski and Davenport-Cassels, this implies that \( ab - e^2 \) is the sum of three integer squares. QED

This finally provides a likely criterion for determining when admissibility is sufficient in \( \mathbb{Z}^4 \), which is supported by computer computations. However, it remains to show that \( ab - e^2 \) being the sum of three squares guarantees that an embedding does exist. The inspiration for this proof comes from noticing the form obtained: \( ab = e^2 + r_1^2 + r_2^2 + r_3^2 \). This number may be interpreted either as the norm of a vector in \( \mathbb{Z}^4 \) or as the norm of an integer quaternion. Due to the importance of quaternions in generating the matrices \( M_k \) and the apparently critical role which
dimension $n = 4$ plays in the problem, it is reasonable to explore what more can be learned from them.

3.3 Quaternions

Define the integer quaternions to be the set of elements $\{a_1 + a_2i + a_3j + a_4k \mid a_i \in \mathbb{Z}\}$. This is a ring with the relations $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$. For the rest of this section, let $A = a_1 + a_2i + a_3j + a_4k$. Then $\overline{A}$ is defined to be $a_1 - a_2i - a_3j - a_4k$. Also, the norm of $A = N(A) = A\overline{A}$ can be computed as $a_1^2 + a_2^2 + a_3^2 + a_4^2$.

Now a one-to-one correspondence exists between the vectors in $\mathbb{Z}^4$ and the integer quaternions, expressed by the relationship $[w_1, w_2, w_3, w_4] \leftrightarrow w_1 + w_2i + w_3j + w_4k$.

Then the vector norm on the left and the quaternion norm on the right both equal $w_1^2 + w_2^2 + w_3^2 + w_4^2$.

Hence the problem of finding $X$ and $Y$ with norms $a$ and $b$, where $XY = e$ and $ab - e^2 = r_1^2 + r_2^2 + r_3^2$ translates into finding two integer quaternions $A$ and $B$ with norms $a$ and $b$ where $AB = e + r_1i + r_2j + r_3k$.

This section is devoted to showing that such an $A$ and $B$ exist, in the spirit of a similar argument given by Pall. Essentially, this amounts to showing that any given integer quaternion can be divided into factors based on the corresponding factors of the norms involved.

Call $B$ a right divisor of $A$ if there exists an integer quaternion $C$ such that $A = CB$. Also $A$ is a multiple of the integer $m$ if $m$ divides $a_1, a_2, a_3$ and $a_4$. Similarly $A \equiv B \mod m$ if $A - B$ is a multiple of $m$. Several useful lemmas are established first in order to simplify the problem.

**Lemma 3.6** If $A \equiv B \mod m$ then $A$ and $B$ have the same set of right divisors with norm $m$. 
Proof: Suppose $B = CD$, with $|D| = m$. Since $A \equiv B \mod m$, there must exist $E$ such that $A = B + mE$. Then $A = (C + E \overline{D})D$. QED

**Lemma 3.7** If $|A|$ is relatively prime to $m$, then $B$ and $AB$ have the same set of right divisors of norm $m$.

Proof: For the forward direction, if $B = CD$ with $|D| = m$, then $AB = (AC)D$ is trivial. Alternatively, suppose $AB = CD$ with $|D| = m$. Since $|A|$ is relatively prime to $m$, there exists an integer $k$ such that $k|A| \equiv 1 \mod m$. Then $k\overline{A}AB = k|A|B \equiv B$, and thus $B \equiv k\overline{A}CD$. Now, by Lemma 3.6, the proof is done. QED

The process will be to take an integer quaternion of norm $n$, and split off factors of prime norm $p$ one at a time, until the product of all of these factors has the norm $m$ that is desired. As usual, the case $p = 2$ requires special consideration and hence will be handled first.

**Lemma 3.8** Suppose $A$ is an integer quaternion with even norm. Then it has a right divisor of norm 2.

Proof: By Lemma 3.6, only a few cases need to be considered.

Case 1: Suppose $a_1 \equiv a_2 \equiv a_3 \equiv a_4 \equiv 0 \mod 2$. Then clearly 2 is a right factor of $A$, and $2 = (1 + i)(1 - i)$.

Case 2: Suppose without loss of generality that $a_1 \equiv a_2 \equiv 1 \mod 2$ and $a_3 \equiv a4 \equiv 0 \mod 2$. Then $A \equiv a_1 + a_2i \mod 2 \equiv 1 + i$, and hence by Lemma 3.6 has a right factor of $1 + i$.

Case 3: Suppose $a_1 \equiv a_2 \equiv a_3 \equiv a_4 \equiv 1 \mod 2$. Then $A \equiv 1 + i + j + k \mod 2$, where the latter factors as $(1 + i)(1 + j)$. Hence, by Lemma 3.6, $A$ has a right factor of $1 + j$. QED

Now, consider the remaining primes. Define an integer quaternion $A$ to be pure mod $p$ if $a_1 \equiv 0 \mod p$. The next lemma further reduces the number of forms for $A$ which must be examined in the final part of the proof.
Lemma 3.9  Let $p$ be an odd prime and let $A$ be an integer quaternion with norm divisible by $p$ and $\gcd(p,a_1,a_2,a_3,a_4) = 1$. Then there exists a pure integer quaternion $B$ such that $BA$ is pure mod $p$ and $|B|$ is relatively prime to $p$.

Proof: The conditions given for $A$ ensure that at least two of the $a_i$ are not divisible by $p$. Assume without loss of generality that $a_2$ is one of these two.

Now write $B$ as $b_1 + b_2i + b_3j + b_4k$. That $BA$ is pure mod $p$ is equivalent to the statement that $a_2b_2 + a_3b_3 + a_4b_4 \equiv 0 \pmod{p}$, or that $b_2 \equiv -a_3/a_2 \cdot b_3 - a_4/a_2 \cdot b_4 = c_3b_3 + c_4b_4$.

Next, $|B|$ relatively prime to $p$ implies that $b_2^2 + b_3^2 + b_4^2 \not\equiv 0 \pmod{p}$, or on substituting the relationship just established for $b_2$, that $(1 + c_3^2)b_3^2 + 2c_3c_4b_3b_4 + (1 + c_4^2)b_4^2 \not\equiv 0$. Now, since $p$ is an odd prime, all three of the terms $(1 + c_3^2), 2c_3c_4$ and $(1 + c_4^2)$ can not all simultaneously be congruent to 0. Thus, there is at least one solution to the last equation, which gives rise to a suitable choice for $B$. QED

So consider an integer quaternion $A$ and an odd prime $p$ which divides the norm of $A$. Showing that a right factor of $A$ with norm $p$ exists proceeds by using Lemma 3.9 to multiply $A$ by an integer quaternion $B$ such that $AB$ is pure mod $p$ while $p \nmid |B|$. By Lemma 3.7, the set of right factors of $A$ and $AB$ are the same. By Lemma 3.6, the real coefficient of $AB$ may be eliminated, also without changing the set of factors. Thus, only values of $A$ in the form $a_2i + a_3j + a_4k$ need to be examined. Now, if $p$ divides $a_2, a_3$ and $a_4$, then trivially there is a right factor of $p$. Otherwise, assume without loss of generality that $p \nmid a_2$. Then there is an integer $k$ such that $ka_2 \equiv 1 \pmod{p}$. Clearly $k$ is relatively prime to $p$, so applying Lemmas 3.7 and 3.6 again reduces the problem to studying the case where $A = i + a_3j + a_4k$. This form is then the subject of the final lemma.

Lemma 3.10  If $A = i + a_3j + a_4k$ has norm a multiple of $p$, then it has a right factor of norm $p$. 

Proof: The goal is to write $A$ as $BC$ where $|C| = p$. Note that this is equivalent to finding a solution $A\overline{C} \equiv 0 \mod p$ with $|C| = p$. For if $A = BC$, then $A\overline{C} = BC\overline{C} = Bp \equiv 0$. And alternatively, if $A\overline{C} = B \equiv 0$, then $B = pD$ and $A\overline{C}C = pA = BC = pDC$, so $A = DC$.

Since $p \mid |A|$, let $1 + a_3^2 + a_4^2 = pk$. Writing $C = c_1 + c_2i + c_3j + c_4k$, the equation $A\overline{C} \equiv 0$ gives four congruences:

\[
\begin{align*}
    c_2 + a_3c_3 + a_4c_4 &\equiv 0 \\
    c_1 + a_3c_4 - a_4c_3 &\equiv 0 \\
    a_3c_1 + a_4c_2 - c_4 &\equiv 0 \\
    a_4c_1 + c_3 - a_3c_2 &\equiv 0
\end{align*}
\]

Using that $1 + a_3^2 + a_4^2 \equiv 0$, these equations reduce to the two congruences $c_1 \equiv a_4c_3 - a_3c_4$ and $c_2 \equiv -a_3c_3 - a_4c_4$. Thus, the target is a solution to $c_1^2 + c_2^2 + c_3^2 + c_4^2 = p$ where $c_1 = a_4C_3 - a_3C_4 + pC_1$, $c_2 = -a_3C_3 - a_4C_4 + pC_2$, $c_3 = C_3$ and $c_4 = C_4$. Substituting these values in, dividing by $p$, and collecting terms results in the equation $p(C_1^2 + C_2^2) + 2(a_4C_1C_3 - a_3C_1C_4 - a_3C_2C_3 - a_4C_2C_4) + (1 + a_3^2 + a_4^2)p \cdot (C_3^2 + C_4^2) = 1$. The quadratic form on the left has a matrix representation as

\[
\begin{bmatrix}
    p & 0 & a_4 & -a_3 \\
    0 & p & -a_3 & -a_4 \\
    a_4 & -a_3 & k & 0 \\
    -a_3 & -a_4 & 0 & k
\end{bmatrix}
\]

with determinant $(pk - a_3^2 - a_4^2)^2 = 1$. Since it is a positive definite quaternary quadratic form of determinant 1, it is equivalent to the form $X_1^2 + X_2^2 + X_3^2 + X_4^2 = 1$, hence has a solution over the integers. QED

Therefore, the desired theorem follows.
**Theorem 3.11** An integer quaternion \( e + r_1i + r_2j + r_3k \) with norm \( ab \) may be factored into the product of two integer quaternions \( A \) and \( B \) with norms \( a \) and \( b \) respectively.

*Proof:* Factor \( b \) into a product of primes. For each 2 which appears, apply Lemma 3.8 to split off a factor of norm 2. For each odd prime \( p \), apply Lemmas 3.9 and 3.10 as necessary to obtain a factor of norm \( p \). Since norms are multiplicative, multiplying all these factors together yields a factor of norm \( b \), and must leave behind the complementary factor of norm \( a \). QED

### 3.4 Embeddability in \( \mathbb{Z}^4 \)

The information gathered in the last few sections is summarized by the following theorem.

**Theorem 3.12** Consider the lattice \( \mathbb{Z}^n \) with \( n = 4 \). If a triple \( (a, b, e) \) is admissible, then the following are equivalent:

i) There are solutions to Equations 2.1 over \( \mathbb{R} \) and \( \mathbb{Z}_p \) for all primes \( p \).

ii) \( ab - e^2 > 0 \) and there is a solution to Equations 2.1 over \( \mathbb{Z}_2 \).

iii) \( ab - e^2 \) can be written as the sum of three integer squares.

iv) The triangle represented by \( (a, b, e) \) can be embedded into \( \mathbb{Z}^4 \).

*Proof:* (i \( \rightarrow \) ii) Since \( ab - e^2 > 0 \) is the condition for the associated triangle to be embeddable in the reals and Theorem 3.2 guarantees solutions in \( \mathbb{Z}_p \) for \( p \) odd, this is trivial.

(ii \( \rightarrow \) iii) This is Lemma 3.5.

(iii \( \rightarrow \) iv) Let \( ab - e^2 = r_1^2 + r_2^2 + r_3^2 \). By Theorem 3.11, there are integer quaternions \( A \) and \( B \) of norms \( a \) and \( b \) respectively, such that \( AB = e + r_1i + r_2j + r_3k \). Then translating \( A \) into a vector \( X \) and \( B \) into a vector \( Y \) via taking the coordinates to
be the real, \( i, j \) and \( k \) components yields vectors of norm \( a \) and \( b \) whose dot product equals \( e \). That is, \( X \) and \( Y \) gives an embedding of the triangle into \( \mathbb{Z}^4 \).

(iv \( \rightarrow \) i) This is trivial. QED

Now a natural question to ask is how many different ways a triangle may be embedded into \( \mathbb{Z}^4 \). Following the method of proof, it is clear that each way of writing \( \Delta = ab - e^2 \) as a sum of three squares results in a different way of writing the corresponding integer quaternion \( e + r_1 i + r_2 j + r_3 k \). Each of these integer quaternions must necessarily give rise to different factorizations into \( A \)'s and \( B \)'s, which in turn result in different choices for \( X \) and \( Y \), giving different embeddings of the triangle into \( \mathbb{Z}^4 \).

Thus, a lower bound on the number of ways of writing \( \Delta \) as the sum of three squares also gives a lower bound on the number of embeddings of the corresponding triangle in \( \mathbb{Z}^4 \). Just such an estimate is given by Siegel:

**Lemma 3.13 (Siegel)** *Suppose \( \Delta \) can be written as the sum of three squares. Then the number of unique ways of writing \( \Delta \) as such a sum is \( r_3(\Delta) \gg \epsilon \Delta^{1/2-\epsilon} \).*

With this analysis complete, the question of embedding triangles in \( \mathbb{Z}^5 \) may now be studied.
Chapter 4

Characterization of Triangles in $\mathbb{Z}^5$

Computational evidence suggests that every admissible triangle may be embedded into $\mathbb{Z}^5$; the goal of this chapter is to prove that conjecture, and to provide asymptotic estimates on the number of embeddings. These asymptotics then become instrumental in proving the equidistribution of rational points on certain manifolds.

4.1 Embedding into $\mathbb{Z}^5$

The fundamental idea is to take an admissible triple $(a, b, e)$ and consider if the corresponding triangle is already embeddable into $\mathbb{Z}^4$. If it is not, then a slight modification should be possible which will reduce the triple to another one $(a', b', e')$ which is known to be embeddable. By choosing this modification carefully, the resulting triangle can then be brought back to an embedding for the original one in $\mathbb{Z}^5$.

The focus shall be on the criterion that a triangle is embeddable into $\mathbb{Z}^4$ if and only if $\Delta = ab - e^2$ can be written as the sum of three squares. By Dirichlet, a number is the sum of three squares exactly when it is nonnegative and not of the form $4^l(8k - 1)$. Since a triangle embeddable in $\mathbb{Z}^4$ is trivially embeddable in $\mathbb{Z}^5$, only $\Delta$s which are of this type need to be studied.

Let $X = [x_1, x_2, x_3, x_4, x_5]$ and $Y = [y_1, y_2, y_3, y_4, y_5]$, with $X^2 = a$, $Y^2 = b$, $XY = e$. The goal will generally be to show that for appropriate choices of $x_5$ and $y_5$, the resulting triangle characterized by $(a - x_5^2, b - y_5^2, e - x_5y_5)$ is embeddable into $\mathbb{Z}^4$. 
say with vectors $X'$ and $Y'$. Then, taking $X = [X', x_5]$ and $Y = [Y', y_5]$ would solve the original problem.

Let $U(r, s) = r^2b - 2rse + s^2a$ for a given choice of $(a, b, e)$. Then $\Delta' = (a - x_5^2)(b - y_5^2) - (e - x_5y_5)^2 = \Delta - U(x_5, y_5)$. It only remains to show that $\Delta'$ is the sum of three squares.

To reduce the complexity of the problem, a few reductions are in order. First, as in Theorem 2.8, it is possible to shift a triangle until it is in the form of either a right or acute triangle, without changing its embeddability or the value of $\Delta$. Order the sides such that $c \leq b \leq a$; in this form, several restrictions on the relative values of $a, b, e$ and $\Delta$ become apparent. First of all, $b \geq c$ implies that $e = (a + b - c)/2$ is at least $a/2$. Also, the Law of Cosines shows that since the angle opposite the side represented by $a$ is acute, then $e \leq b$. Therefore, the system of inequalities $a/2 \leq e \leq b \leq a \leq 2e \leq 2b$ holds; hence bounding any one of these three numbers is sufficient to bound the collection of triangles under consideration.

The next couple of Lemmas are designed to provide an effective bound on the relationship between $(a, b, e)$ and $\Delta$, thereby providing some flexibility in the choices for $x_5$ and $y_5$ in the following theorem. Note that in the following proofs, lower bounds for $b$ are implicitly or explicitly assumed. In each case, if $b$ is less than these bounds, then all the associated triangles have been computed directly and shown to be embeddable (in particular, all triangles with $1 \leq b \leq a \leq 500$ have been examined).

**Lemma 4.1** If $\Delta = 0$, then the triangle is degenerate, but may be ‘embedded’ in $\mathbb{Z}^4$.

**Proof:** Since $\Delta = 0$, it follows that $e = \sqrt{ab}$ and hence $ab = e^2$ must be a perfect square. Write $a = \alpha^2m$ and $b = \beta^2n$ where $m$ and $n$ are squarefree. Since $ab$ is a perfect square, it follows that $m = n$. Let $m = m_1^2 + m_2^2 + m_3^2 + m_4^2$; then
taking \( X = [\alpha m_1, \alpha m_2, \alpha m_3, \alpha m_4] \) and \( Y = [\beta m_1, \beta m_2, \beta m_3, \beta m_4] \) gives the desired embedding. QED

**Lemma 4.2** If \( a \geq \Delta \), then the triangle characterized by \((a, b, e)\) may be embedded into \( Z^5 \).

**Proof:** If \( a = \Delta \), then the triple \((a, b-1, e)\) which comes from assuming \( x_5 = 0 \) and \( y_5 = 1 \) has \( U(0, 1) = a \) and thus \( \Delta' = 0 \). Then by the prior lemma it represents a triangle embeddable in \( Z^4 \), and therefore \((a, b, e)\) represents a triangle in \( Z^5 \).

Otherwise \( a > \Delta \), and thus \( b > \Delta/2 \). Therefore \( \Delta = ab - e^2 \geq ab - b^2 = b(a-b) > \Delta(a-b)/2 \). Thus \( a-b < 2 \), so \( a = b \) or \( a = b + 1 \). A further restriction stems from considering \( e \); namely if \( e < b - 1 \) then \( e^2 < a(b-1) \) is trivial. Thus \( b - 1 \leq e \leq b \), and there a total of four possible types of triples to consider.

First suppose \( a = b = e \); then \( \Delta = 0 \) and the triangle is embeddable. Similarly if \( a = b + 1 \) and \( e = b \), then \( \Delta = b = U(1, 0) \) and \( \Delta' = 0 \) for the modified triple \((a-1, b, e)\).

Then suppose \( e = b - 1 \). If \( a = b \) then \( U(1, 1) = 2 \) and \( \Delta' = \Delta - 2 \) for the modified triple \((a-1, b-1, e-1)\). Since it is impossible for both \( \Delta \) and \( \Delta - 2 \) to be of the form \( 4^l(8k - 1) \), either \((a, b, e)\) corresponds to a triangle embeddable in \( Z^4 \), or else \((a-1, b-1, e-1)\) does. In either case, \((a, b, e)\) gives a triangle embeddable in \( Z^5 \).

Finally consider \( a = b + 1 = e + 2 \). Then \( U(1, 1) = 3 \) and \( U(2, 2) = 12 \). As before, it is impossible for all the values \( \Delta, \Delta - 3 \) and \( \Delta - 12 \) to be of the form \( 4^l(8k - 1) \). The rest of the proof follows as before.

Note that the implicit assumption that \( \Delta \geq 12 \) is not a problem, since the first value of \( \Delta \) for which \( \Delta \) and \( \Delta - 3 \) are both problematic is 31. QED

The primary benefit of this last lemma was to show that bounding \( \Delta \) also serves to bound the problematic values of \( a \). The next lemma lowers this ratio even further.
Lemma 4.3 If \( a \geq \Delta/4 \), then the triangle characterized by \((a, b, e)\) may be embedded into \( \mathbb{Z}^5 \).

**Proof:** As in the last proof, if \( a = \Delta/4 \), then the triple \((a, b - 4, e)\) gives a degenerate triangle, which is ‘embeddable’ in \( \mathbb{Z}^4 \).

Otherwise \( a > \Delta/4 \). Then \( \Delta' < 0 \) for the triple \((a, b - 4, e)\), which in turn requires \( e^2 > a(b - 4) \). However, if \( e \leq b - 4 \) this situation can not arise; thus the finite number of cases where \( e = b - i, 0 \leq i \leq 3 \) must be examined.

**Case 1:** Assume that \( i = 0 \), so \( e = b \), and write \( a = b + k \). Then \( \Delta' < 0 \) implies that \( e^2 = b^2 > (b + k)(b - 4) = b^2 + (k - 4)b - 4k \), or that \( 4k > (k - 4)b \). Then \( k < 4b/(b - 4) = 4 + 16/(b - 4) \). The cases where \( b < 20 \) can be computed directly, so assume that \( k \leq 4 \).

If \( k = 0 \) then \( a = b = e \), so \( \Delta = 0 \). By Lemma 4.1, this case is always embeddable.

If \( k = 1 \) then \( a = b + 1 \) and hence \( b = \Delta \). Then \((a - 1, b, e)\) is degenerate and embeddable in \( \mathbb{Z}^4 \).

For \( k = 2 \), \( U(1, 1) = 2 \) and both \( \Delta \) and \( \Delta - 2 \) can not be of the form \( 4^l(8k - 1) \).

Finally, if \( k = 3 \) then \( U(1, 1) = 3 \) and \( U(2, 2) = 12 \). Again, not all of \( \Delta \), \( \Delta - 3 \) and \( \Delta - 12 \) can be problematic.

**Case 2:** Now \( i = 1 \) and \( e = b - 1 \). Writing \( a \) as \( b + k \) and proceeding as before leads to the conclusion that \( k \leq 2 \) for \( b \geq 13 \). For \( a = b \), consider \( U(1, 1) = 2 \) and proceed as before. Similarly for \( a = b + 1 \) it follows that \( U(1, 1) = 3 \) and \( U(2, 2) = 12 \).

Finally, for \( a = b + 2 \) it must be noted that \( \Delta = ab - e^2 = (b + 2)b - (b - 1)^2 = 4b - 1 \). Hence \( \Delta \equiv 3, 7 \mod 8 \), and only the latter possibility is a concern. But then \( U(1, 1) = 4 \) and \( \Delta - 4 \equiv 3 \mod 8 \) leads to a triangle embeddable in \( \mathbb{Z}^4 \).

**Case 3:** Next is \( e = b - 2 \). Now the process yields \( k = 0 \) for \( b \geq 8 \), and thus the triple \((b, b, b - 2)\) is under examination. To see that this one is embeddable, consider \( c = a + b - 2e = U(1, 1) = 4 \). Then the value of \( e' \) is \((b + c - a)/2 = 2 \), and
working with \((b, 4, 2)\) is equivalent to working with \((a, b, e)\). However, the triangle associated to \((b, 4, 2)\) can be embedded readily by taking \(X = [1, \beta_1, \beta_2, \beta_3, \beta_4]\) and \(Y = [2, 0, 0, 0, 0]\) where \(\beta_1^2 + \beta_2^2 + \beta_3^2 + \beta_4^2 = b - 1\).

\[\text{Case 4:}\] Finally \(e = b - 3\). This time \(k < 0\) (that is no possible problems exist) for \(b \geq 5\). \(\text{QED}\)

With this preliminary work done, proving the main theorem of this chapter is straightforward.

**Theorem 4.4** If \((a, b, e)\) is admissable, then the associated triangle is embeddable into \(\mathbb{Z}^5\).

**Proof:** If \(\Delta\) is not of the form \(4^l(8k - 1)\), then the triangle is already embeddable in \(\mathbb{Z}^4\). Therefore, assume that it is of this form, and proceed by cases on the value of \(l\). Furthermore, the assumption that the triangle has been reduced to a non-obtuse form remains in effect. Since Lemma 4.3 takes care of the cases where \(a \geq \Delta/4\) it will also be assumed that \(a < \Delta/4\).

\[\text{Case 1:}\] Suppose that \(l = 0\), hence \(\Delta = 8k - 1\) for some choice of \(k\). Then \(U(1, 0) = b\) implies that if \(b \equiv 1, 2, 4, 5, 6\) mod 8 then \(\Delta - U(1, 0) \not\equiv 0, 4, 7\) mod 8, therefore \(\Delta - U(1, 0)\) can not be of the form \(4^m(8n - 1)\). So then for these choices of \(b\), \((a - 1, b, e)\) is embeddable in \(\mathbb{Z}^4\).

Similarly, if \(b \equiv 3, 7\) then \(U(2, 0) = 4b \equiv 4\) mod 8. Then \(\Delta - U(2, 0) \equiv 3\) mod 8, and as before, this implies that \((a - 4, b, e)\) is embeddable in \(\mathbb{Z}^4\).

This leaves the only problematic choice for \(b\) to be \(b \equiv 0\) mod 8. By a symmetric argument, assume also that \(a \equiv 0\) mod 8. Then \(ab - e^2 \equiv 7\) mod 8 implies that \(e\) is odd. Therefore \(U(1, 1) \equiv \pm 2\) mod 8 and thus \(\Delta - U(1, 1) \equiv 1, 5\) mod 8, showing that \((a - 1, b - 1, e - 1)\) is embeddable in \(\mathbb{Z}^4\).
Case 2: Suppose that $l = 1$, hence $\Delta = 4(8k - 1) \equiv 4 \mod 8$. Now if $b \equiv 1, 2, 3, 6, 7$, then $\Delta - U(1, 0) \not\equiv 0, 4, 7 \mod 8$, and thus $(a - 1, b, e)$ is embeddable in $\mathbb{Z}^4$.

If $b \equiv 4, 5 \mod 8$, then $\Delta - U(2, 0) = 4(8k - 1) - 4b = 4(8k - 1 - b)$, which is not of the form $4^m(8n - 1)$, hence $(a - 4, b, e)$ is embeddable in $\mathbb{Z}^4$.

This leaves the case where $b = 8\beta$; again by symmetry let $a = 8\alpha$. This then requires that $e = 4\epsilon + 2$. Then $\Delta - U(2, 2) = 4(8k - 1) - 32\alpha - 32\beta + 8(4\epsilon + 2) = 4(8k - 1 - 8\alpha - 8\beta + 8\epsilon + 4) = 4(8k' + 3)$. Thus, $(a - 4, b - 4, e - 4)$ is embeddable in $\mathbb{Z}^4$.

Case 3: Finally suppose that $l \geq 2$, hence $\Delta \equiv 0 \mod 8$. Then $\Delta - U(1, 0) = 4^l(8k - 1) - b$ is not of the form $4^m(8n - 1)$ if $b \equiv 2, 3, 5, 6, 7 \mod 8$. Similarly, if $a$ is congruent to one of these numbers, then $\Delta - U(0, 1)$ is the sum of three squares. Finally, since $c = U(1, 1)$, the same result applies to $c$.

Therefore, the only problematic case to consider is when $a, b$ and $c$ are all 0, 1 or 4 mod 8. First consider $a$; if $a$ is a multiple of 4, then $e$ is even and it is possible to reduce the problem to considering the triple $(a/4, b, e/2)$. An embedding of the new triangle may be restored to an embedding of the original by doubling all the entries in the $X$ vector. The value of $\Delta'$ is then $\Delta/4$. This reduction may be repeated until either the power of 4 in $\Delta'$ is lowered to 1 (and Case 2 then completes the process), or $a$ has no more factors of 4 remaining. Then if $a$ is not 1 mod 8 the initial argument gives an embedding for the reduced triangle.

Otherwise, $a$ has been reduced to a number which is 1 mod 8 and $\Delta$ still is of the form $4^l(8k - 1)$ with $l \geq 2$. Then the identical argument may be applied to $b$ to either embed the triangle or to also reduce $b$ to a number which is 1 mod 8. Relabel $a$ and $b$ to be their reduced counterparts for simplicity. Since $a \equiv b \equiv 1 \mod 8$, it follows that $e \equiv 1 \mod 2$ and then that $c$ is a multiple of 4.
Now, change to considering the embedding in terms of \((b, c, e')\). Apply the same reduction to \(c\) until either a triangle known to be embeddable is found, or until \(c\) is reduced to 1 mod 8. Then \(e' = (b + c - a)/2\) can not be an integer. However, the assumptions before the reduction is performed are that \(c\) is a multiple of 4 and \(\Delta\) is 0 mod 8, hence \(e'\) must have been even. Therefore, the process can not continue to the point where \(c\) is 1 mod 8, hence it must terminate at some point with an embeddable triangle.  \(QED\)

Thus the necessary conditions are also sufficient for \(n \geq 5\).

4.2 Number of embeddings

Now, the question of how many different ways a triangle may be embedded into \(\mathbb{Z}^5\) should be addressed. Simply allowing \(\Delta\) to go off to infinity is not sufficient however. Consider the situation where \(\Delta\) is replaced by 4\(\Delta\); here it is likely that embedding triangles will require the reduction argument given in the latter part of Theorem 4.4. The process essentially eliminates powers of 4 without introducing the potential for new triangles. This is analogous to the problem of finding lattice points on spheres in \(\mathbb{R}^4\) - multiplying the radius of the sphere by a factor of 4 does not introduce any new lattice points.

Therefore, the asymptotics in this section shall be based on a fixed \((a, b, e)\) triple, which shall be scaled up by odd factors \(\lambda\) to triples \((\lambda a, \lambda b, \lambda e)\). Noting that since the shifting process used to reduce a triangle to a non-obtuse form is invertible, it follows that there are exactly as many embeddings of the triangle given by \((a, b, e)\) as there are of the triangle given by the reduced form \((a', b', e')\). This in particular allows the assumption that \(e \geq b/2 > 0\).
The aim is to show that there are at least $C\lambda^{2-\epsilon}$ distinct embeddings of the triangle given by $(\lambda a, \lambda b, \lambda e)$ into $\mathbb{Z}^5$, where $C$ is a constant determined by $a, b, e$ and $\epsilon$. The analysis shall proceed by following the proof of Theorem 4.4.

First, note that while $a, b$ and $e$ increase by a factor of $\lambda$, $\Delta$ increases by a factor of $\lambda^2$. Since it is being assumed that $\lambda$ is odd, then $\lambda^2 \equiv 1 \mod 8$, so $\Delta$ remains unchanged mod 8, and the power of 4 does not change if $\Delta$ is of the form $4^l(8k - 1)$. In addition, $a$ can not remain greater than $\Delta/4$ for more than a finite number of values of $\lambda$, hence the proofs of Lemmas 4.2 and 4.3 do not need to be revisited.

**Theorem 4.5** Consider an embeddable triangle, and let its non-obtuse reduced form be characterized by the triple $(a, b, e)$. Then for $\lambda$ odd and sufficiently large, the number of distinct ways to embed the triangle into the lattice $\mathbb{Z}^5$ is at least $C\lambda^{2-\epsilon}$. The constant $C$ only depends on the values of $a, b$ and $e$, and the choice of $\epsilon$.

**Proof:** This proof shall also be primarily concerned with projecting the problem down a dimension, and finding many associated embeddings in $\mathbb{Z}^4$. Consider the triple $(\lambda a, \lambda b, \lambda e)$ with $\Delta = \lambda^2(ab - e^2)$. The first thing to estimate is the number of choices for $r$ and $s$ such that $\Delta - U(r, s) > 0$.

Since $U(r, s) = r^2\lambda b + s^2\lambda a - 2rs\lambda e$, an upper bound of $\lambda(r^2b + s^2a)$ will be sufficient. The question then is how many values of $(r, s)$ may be chosen such that $r^2b + s^2a < \lambda(ab - e^2)$. These possible values are lattice points in the first quadrant while lie inside the ellipse governed by the inequality. The number of such points may be estimated by the area inside the curve. As $\lambda$ increases, the major and minor axes increase as $\sqrt{\lambda}$, and thus the area increases as $\lambda$ as well.

By including in a factor of $\frac{1}{2}$ so that $r^2b + s^2a < \lambda(ab - e^2)/2$, it can similarly be shown that there are on the order of $\lambda$ choices for $(r, s)$ such that $\Delta' = \Delta - U(r, s) > \Delta/2$. Recalling Lemma 2.5 which gives $C\epsilon\Delta^{1/2-\epsilon}$ or $C'\lambda^{1-\epsilon}$ embeddings of a triangle into $\mathbb{Z}^4$, it only remains to show that a fixed proportion of the values for $(r, s)$ give
rise to triangles that can be so embedded. For then there would be at least $C_1 \lambda$ choices for $(r, s)$ which all give at least $C_2 \lambda^{1-\epsilon}$ triangles; any particular triangle may show up on this list a bounded number of times, giving a final total of $C\lambda^{2-\epsilon}$ distinct embeddings into $\mathbb{Z}^5$.

To find this fraction of values for $(r, s)$, consider the value of $ab - e^2$.

**Case 1:** If $ab - e^2$ is 1, 2, 3, 5 or 6 mod 8, then any acceptable values for $r$ and $s$ which are also multiples of 4 will do. For then $8 \mid U(r, s)$ and thus $\lambda^2(ab - e^2) - U(r, s) \equiv ab - e^2 \mod 8$ will be the sum of three squares.

**Case 2:** Now suppose $ab - e^2 \equiv 4 \mod 8$. If $\lambda b \equiv 1, 2, 3, 6, 7 \mod 8$, then $\lambda^2(ab - e^2) - U(1 + 8m, 8n) \equiv (ab - e^2) - \lambda b \mod 8$, and hence can not be of the form $4^l(8k - 1)$. Thus at least $1/64^{th}$ of the values for $r$ and $s$ will be acceptable.

In the case that $\lambda b \equiv 4, 5 \mod 8$, greater attention must be paid to the factorization of $ab - e^2$. If $ab - e^2 = 4(8k - 1)$, let $r = 2 + 8m$ and $s = 8n$. Then $\lambda^2(ab - e^2) - U(r, s) = 4(8k' - 1) - 64n^2\lambda a - (4 + 32m + 64m^2)\lambda b + 2(2 + 8m)8n\lambda e = 4(8k' - 1 - 16n^2\lambda a - \lambda b - 8m\lambda b - 16m^2\lambda b + (1 + 4m)8n\lambda e) = 4(8k'' - 1 - \lambda b)$, which is the sum of three squares.

Alternatively, $ab - e^2 = 4(8k + \delta)$, where $\delta$ is 1, 2, 3, 5 or 6. Then take $r = 8m$ and $s = 8n$; thus $\lambda^2(ab - e^2) - U(r, s) = 4(8k' + \delta) - 64m^2\lambda b - 64n^2\lambda a + 128mn\lambda e = 4(8k' + \delta - 16m^2\lambda b - 16n^2\lambda a + 32\lambda e) = 4(8k'' + \delta)$, which also is the sum of three squares.

Since a similar argument holds for $\lambda a$ as well, assume that $\lambda a = 8\alpha$ and $\lambda b = 8\beta$. Then $\lambda e$ must be of the form $4\epsilon + 2$. Taking $r = 2 + 8m$ and $s = 2 + 8n$ and proceeding as before now yields $\lambda^2(ab - e^2) - U(r, s) = 4(8k' + 3)$, which is sufficient.

**Case 3:** Now $ab - e^2$ is $4^l(8k + \delta)$, where $\delta$ is 1, 2, 3, 5, 6 or 7. If $\lambda b \equiv 2, 3, 5, 6, 7 \mod 8$, then taking $r = 1 + 8m$ and $s = 8n$ and using the above argument is sufficient. This process works for $\lambda a$ in the corresponding way.
Now, if $\lambda a \equiv 1, 4 \mod 8$, take $r = 2^l + 2^{l+3}m$ and $s = 2^{l+3}n$. Since $l$ is a constant based on $a, b$ and $e$, this will still give a fixed proportion of the choices for $r$ and $s$. As before, this results in $\lambda^2(ab - e^2) - U(r, s) = 4^l(8k'' - 1 - b)$, which is the sum of three squares.

Thus the only remaining case is $\lambda a \equiv \lambda b \equiv 0 \mod 8$. Since $\lambda$ is assumed to be odd, this means $a \equiv b \equiv 0 \mod 8$. This also means that $e$ is a multiple of 4. Then factor out multiples of 4 until $a$ and $b$ are not both multiples of 8, or $ab - e^2$ is not a multiple of 8. Therefore, at the cost of a decrease in the constant $C$, the problem is reduced to an earlier case while maintaining the order of $\lambda^{2-\epsilon}$ embeddings. \textbf{QED}
Chapter 5

Analytic Methods

A homogenized version of the problem arises by considering what rational scalings of a triangle may be embedded into \( \mathbb{Z}^n \). In particular, for a given admissible triple \((a, b, e)\), consider all other triples \((\lambda a, \lambda b, \lambda e)\) where \( \lambda \in \mathbb{Q} \) and \( \lambda a, \lambda b, \lambda e \in \mathbb{Z} \). Clearly, if the former is admissible, so are the latter. Furthermore, this defines an equivalence relation amongst the set of triangles; denote an equivalence class by \([a, b, e]\).

The question is then to find how many vectors \( X \) and \( Y \) satisfy \((|X|^2, |Y|^2, XY) \in [a, b, e]\). In order to provide useful estimates, a restriction that \(||X||, ||Y|| \leq P\) will be placed on the vectors, where \( ||X|| = \max\{|x_i|, 1 \leq i \leq n\} \) and \( P \) is a positive integer. The analysis will follow the form of the Hardy-Littlewood Method.

5.1 Foundations

For an admissible triple \((a, b, e)\), define \( N_P \) to be the number of choices for vectors \( X \) and \( Y \) in \( \mathbb{Z}^n \) where \((|X|^2, |Y|^2, XY) \in [a, b, e]\) and \(||X||, ||Y|| \leq P\). In other words, \( N_P \) is the number of embeddings of a rational multiple of the triangle represented by \((a, b, e)\) into \( \mathbb{Z}^n \). For simplicity, assume that \( \gcd(a, b, e) = 1 \); scaling does not affect the set \([a, b, e]\) at all, while this assumption forces \( \lambda \) to be an integer if \((a', b', e') = (\lambda a, \lambda b, \lambda e) \in [a, b, e]\).

The first condition on \( X \) and \( Y \) then translates as \(|X|^2 = \lambda a, |Y|^2 = \lambda b\) and \(XY = \lambda e\) for some \( \lambda \in \mathbb{Z} \). Now, this is equivalent to the statement \(|X|^2/a =
$|Y|^2/b = XY/e = \lambda$, which gives rise to the pair of homogenous equations

\[ b|X|^2 - a|Y|^2 = 0 \]
\[ bXY - e|Y|^2 = 0 \]

Suppose $X$ and $Y$ satisfy the first equation. Then $\int_0^1 \exp(2\pi i \alpha (b|X|^2 - a|Y|^2)) \, d\alpha = 1$; otherwise, this integral is 0. Hence, by using versions of this exponential function for both equations and using the characteristic function of the unit $n$ dimensional cube, $N_P$ may be computed as

\[
\int_0^1 \int_0^1 \sum_{X, Y \in \mathbb{Z}^n} \exp(2\pi i (\alpha(b|X|^2 - a|Y|^2) + \beta(bXY - e|Y|^2))) \chi\left(\frac{X}{P}\right) \chi\left(\frac{Y}{P}\right) \, d\alpha \, d\beta
\]

Denote the exponential sum in this expression by $S_n(\alpha, \beta)$. Since $|X|^2 = \sum_{1 \leq i \leq n} x_i^2$ and $XY = \sum_{1 \leq i \leq n} x_i y_i$, and the summation is over all possible vectors $X$ and $Y$, it follows that $S_n(\alpha, \beta) = (S_1(\alpha, \beta))^n$.

To estimate $S_n(\alpha, \beta)$, the problem will be broken down into major and minor arcs. The major arcs $I_\theta$ are those intervals for $(\alpha, \beta)$ which are ‘close’ to a rational point with small denominator. On such intervals, a very good estimate for $S_n(\alpha, \beta)$ is possible. The minor arcs are the complement to $I_\theta$, and here a uniform estimate will be used for $S_n(\alpha, \beta)$ to obtain part of the error term in $N_P$.

### 5.2 Matrix Estimates

The first part of the argument will be to obtain the minor arc contribution to $N_P$. While the traditional Circle Method simply uses a uniform bound to find the error term, it is not quite enough in this problem. In particular, to obtain an estimate smaller than the main term, the function $|S_n(\alpha, \beta)|$ must be decomposed as $|S_1(\alpha, \beta)|^4 |S_{n-4}(\alpha, \beta)|$. Then the savings obtained in computing $|S_1(\alpha, \beta)|^4$ will be sufficient while still applying the uniform bound to $S_{n-4}(\alpha, \beta)$. 


Denote the unit square \([0, 1] \times [0, 1]\) by \(\Pi^2\) and \(S_1(\alpha, \beta)\) by \(S(\alpha, \beta)\); the problem then is to estimate

\[
\int \int_{\Pi^2-I_0} |S(\alpha, \beta)|^4 d\alpha d\beta \leq \int \int_{\Pi^2} |S(\alpha, \beta)|^4 d\alpha d\beta
\]

Now \(|S(\alpha, \beta)|^4 = S_2(\alpha, \beta)S_2(\alpha, \beta)|2\), so integrating this term over \(\Pi^2\) yields the number of solutions to the equations

\[
\begin{align*}
&bQ(X, X) - aQ(Y, Y) = 0 \\
&bQ(X, Y) - eQ(Y, Y) = 0 \\
&||X|| \leq P, ||Y|| \leq P
\end{align*}
\]

where \(Q(X, Y) = x_1y_1 + x_2y_2 - x_3y_3 - x_4y_4\).

Now there is an equivalence between vectors \(X\) and matrices \(A\) given by

\[
(x_1, x_2, x_3, x_4) \rightarrow \begin{bmatrix} x_1 + x_3 & -x_2 - x_4 \\ x_2 - x_4 & x_1 - x_3 \end{bmatrix}
\]

Note that there is a one to one correspondence between integer vectors \(X\) and integer matrices \(A\) with \(A_{11} + A_{22} \equiv A_{12} + A_{21} \equiv 0 \mod 2\). Finally, define the adjoint \(A^*\) by the relationship

\[
A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \leftrightarrow A^* = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}
\]

The usefulness of these matrices follows from the fact that \(Q(X, Y) = \frac{1}{2} \text{tr}(AB^*)\) where \(A\) is the matrix corresponding to \(X\) and \(B\) corresponds to \(Y\). Similarly, \(\det(A) = Q(X, X)\). Then the equations to solve may be transformed into

\[
\begin{align*}
&b\det(A) - a\det(B) = 0 \\
&\frac{b}{2} \text{tr}(AB^*) - e\det(B) = 0 \\
&||A|| \leq 2P, ||B|| \leq 2P
\end{align*}
\]
where \( ||A|| = \max\{|A_{ij}|, 1 \leq i, j \leq 2\} \). Note that \( ||X|| \leq P \rightarrow ||A|| \leq 2P \) and \( ||A|| \leq 2P \rightarrow ||X|| \leq 2P \). Then if \( L_P \) is the number of solutions to the matrix equations it follows that \( N_P \leq L_{2P} \). Since the desired asymptotic estimate will be a power of \( P \), the particular constant will be ignored.

The target is an approximation to the number of matrices appearing in \( L_P \); the next lemma is the beginning of a classification of these matrices.

**Lemma 5.1** Let \( M \) be a 2 by 2 matrix over \( \mathbb{Z} \). Then if \((A, B)\) is a solution to the matrix equations, then, ignoring the norm condition, so is \((AM, BM)\).

**Proof:** This is immediate from computing \( \det(AM) = \det(A) \det(M) \) and \( \text{tr}((AM)(BM)^*) = \text{tr}(AMM^*B^*) = \det(M) \text{tr}(AB^*) \). QED

This then is the analagous result to being able to scale vectors by a length \( \sqrt{k} \) in Lemma 2.5. Now, in order to be able to compute effectively with these matrices, a standard form needs to be established. Define two matrices to be equivalent if there is a matrix \( U \in SL_2(\mathbb{Z}) \) which takes one to the other. Then a particular representative may be chosen from each class of matrices with the next lemma.

**Lemma 5.2** Let \( M \) be a 2 by 2 matrix with integer coefficients such that \( \det(M) \neq 0 \). Then \( M \) is equivalent to an upper triangular matrix \( G \) with \( 0 \leq G_{12} < G_{22} \).

**Proof:** The first step is to turn \( M \) into an upper triangular matrix \( M' \) via a choice of \( U \in SL_2(\mathbb{Z}) \). For simplicity of notation, write \( M \) as \([m_1 \ m_2 \ m_3 \ m_4] \). Let \( d = \gcd(m_1, m_3) \), and take \( u_3 = m_3/d \) and \( u_4 = -m_1/d \). Then \((UM)_{21} \) is 0 by construction. Furthermore, \( \gcd(u_3, u_4) = 1 \), hence there exist integers \( u_1 \) and \( u_2 \) such that \( u_1u_4 - u_2u_3 = 1 \), placing \( U \) in \( SL_2(\mathbb{Z}) \) as desired.

Now let \( M' = UM \). Since \( \det(M') = m'_1m'_4 = \det(M) \neq 0 \), \( m'_4 \neq 0 \). Choose \( l \) such that \( 0 \leq m'_2 - lm'_4 < m'_4 \), and construct \( V \) as \([1 \ -l] \). Then \( V \) is in \( SL_2(\mathbb{Z}) \) and taking \( G = VM' \) gives the final result. QED
Define $A$ to be a right divisor of a matrix $M$ if there exists an integral matrix $B$ such that $M = BA$. Note that if $A$ is a right divisor of $M$, then so is $UA$ for any $U \in SL_2(\mathbb{Z})$. The number of divisors of a matrix with bounded norm will become a major component of the final estimate, hence the next lemmas will be used to approximate that quantity.

**Lemma 5.3** Let $G$ be a matrix in standard form. Then

1. $G \mid W \rightarrow g_1 \mid w_1$.
2. Let $G \mid W$ with $g_1$ and $g_4$ fixed. Then there are at most $h = \gcd(w_1/g_1, g_4)$ possible values for $g_2$.

**Proof:** Part i) follows trivially from matrix multiplication.

For part ii), $G \mid W$ implies that $WG^{-1}$ is an integral matrix with entries $w_1g_4/d, (w_2g_1 - w_1g_2)/d, w_3g_4/d, (w_4g_1 - w_3g_2)/d$, where $d = g_1g_4 = \det(G)$.

Since $w_1g_4/d \in \mathbb{Z}$, it must be the case that $w_1 = w'_1g_1$, and similarly $w_3 = w'_3g_1$. Substituting these forms into the other two relations and cancelling the factors of $g_1$ gives $w'_1g_2 \equiv w_2 \mod g_4$ and $w'_3g_2 \equiv w_4 \mod g_4$.

Now $h$ divides $g_4$ and $w'_1$ by construction, hence it must divide $w_2$ as well. Therefore $w'_1g_2 \equiv w_2 \mod g_4$ reduces to $w''_1g_2 \equiv w'_2 \mod g'_4$, where each term has had a factor of $h$ removed. In addition, $w''_1$ is relatively prime to $g'_4$, hence is invertible $\mod g'_4$. So, $g_2$ satisfies the relationships $g_2 \equiv (w''_1)^{-1}w'_2 \mod g'_4$ and $0 \leq g_2 < g_4$, leaving $g_4/g'_4 = h$ choices for $g_2$. QED

Define a lattice point $(x, y)$ to be primitive if $\gcd(x, y) = 1$. The next lemma provides a bound on the number of primitive lattice points in a certain type of region, based on its area. The specific region that this will be applied to arises in the subsequent lemma.
Lemma 5.4 Let $K$ be a bounded, symmetric, convex region in the $(x, y)$ plane. Then the number of primitive lattice points in $K$ (denoted by $N_K$) is bounded by $2|K| + 2$, where $|K|$ is the area of $K$.

Proof: Only two primitive lattice points may be on any line through the origin ($(x, y)$ and $(-x, -y)$), so consider the set of such lines which go through a nonzero lattice point of $K$. Since $K$ is bounded, this gives a finite collection of lines. Order them in a counterclockwise direction starting from the positive $x$ axis and running to the negative $x$ axis. Since $K$ is symmetric, only $K'$, the upper half of the region, needs to be considered. Also, $K$ is convex, so each line contains exactly one primitive lattice point in $K'$.

Consider the triangle formed by the origin, the primitive lattice point on one line, and the primitive lattice point on the next line. Since all of these points are integral, the area of the triangle must be at least $\frac{1}{2}$. Forming these triangles for each line gives a series of disjoint regions whose total area is equal to at least $\frac{1}{2}$ the number of primitive lattice points in $K'$. Taking the full region $K$ doubles the number of lattice points while also doubling the area, thus $N_K \leq 2|K|$.

This construction fails if there is at most one such line in $K$, however then there are at most 2 primitive lattice points in $K$. Thus, in either case, $N_K \leq 2|K| + 2$.

QED

Lemma 5.5 Let $P > 1$ be fixed, and let $G$ be a matrix in standard form with nonzero determinant. Then the number of matrices $A$ equivalent to $G$ with $||A|| \leq P$ is bounded by $C_\epsilon P^{2+\epsilon}/d$, where $d = \det(G) = g_1 g_4$.

Proof: Let $U$ be in $SL_2(\mathbb{Z})$, fix $j$, and suppose $2^j \leq |u_1| < 2^{j+1}$. Take $A$ to be $UG$, so $a_1 = u_1 g_1, a_2 = u_1 g_2 + u_2 g_4, a_3 = u_3 g_1$ and $a_4 = u_3 g_2 + u_4 g_4$. Since $||A|| \leq P$, it follows that $|u_1 g_1| \leq P$, so $|u_1| \leq \min(2^{j+1}, P/g_1)$. Similarly $|u_1 g_2 + u_2 g_4| \leq P$. 

38
These inequalities for $u_1$ and $u_2$ map out a parallelogram in the $u_1, u_2$ plane which is centered at the origin. Since $\gcd(u_1, u_2) \mid \det(U) = 1$, only the primitive lattice points in this region need to be considered.

The area of the parallelogram is bounded by $C2^jP/g_4$, hence by Lemma 5.4, there are at most $2C2^jP/g_4$ choices for $u_1$ and $u_2$. Next, $u_3$ and $u_4$ must be chosen such that $u_1u_4 - u_2u_3 = 1$. Therefore, $u_3 \equiv -u_2^{-1} \mod u_1$; combined with the requirement that $|u_3| \leq P/g_1$, this gives at most $2^{-j}P/g_1$ choices for $u_3$.

Finally, having chosen $u_1, u_2$ and $u_3$ fixes the value for $u_4$, so there are at most $(C'2^jP/g_4)(2^{-j}P/g_1) = C'P^2/d$ possible matrices $U$ for each choice of $j$. Since at most $\log(P)$ values of $j$ must be considered, the result follows. QED

With these bounds done, the proof of the main theorem for this section will be straightforward. Having translated the vector version of the homogenous equations to matrices, a further change will be made to parameters which can readily be estimated in comparison to $P$, providing a limit on the number of solutions.

**Theorem 5.6** $L_P$, the number of solutions to the matrix equations of norm at most $P$, is bounded by $C_\epsilon P^{4+\epsilon}$.

**Proof:** Suppose $A$ and $B$ are integer matrices which satisfy the equations, with $d = \det(A) \neq 0$. Fix $j$ and suppose $2^j \leq d < 2^{j+1}$; note that since $||A|| \leq P$, $2^{j+1}$ can not exceed $4P^2$.

Let $W = BA^*$; since $A$ and $B$ satisfy the matrix equations, $\det(B) = \frac{b}{a} \det(A)$, and thus $\det(W) = \det(B) \det(A) = \frac{b}{a}d^2$. Similarly, $\det(W) = \frac{2\epsilon}{a}d$. Also, $||W|| \leq P^2$.

The number of solutions $A, B$ is then bounded by the number of choices for $W$ and $A^*$, where $W$ satisfies these relationships and $A^* \mid W$.

Choose a factorization for $d$ as $xy$. There are at most $C_\epsilon d^\epsilon < C'_\epsilon P^\epsilon$ such factorizations. Define $H_{x,y}$ to be the set of matrices $A$ with $A^*$ equivalent to $\begin{bmatrix} \tilde{x} & \ast \\ \tilde{y} & \ast \end{bmatrix}$ and $||A^*|| \leq P$. 
Now for $k$ a fixed integer, a limit to the number of choices for $W$, where $2^k \leq h = \gcd(w_1/x, y) < 2^{k+1}$, is given by $C2^{-k}P^{2+\epsilon}/x$. This follows because of the facts that $|w_1| \leq P^2$, $x|w_1$ (from Lemma 5.3) and $h|\frac{w_1}{x}$ by construction, yielding a total of $C2^{-k}P^2/x$ choices for $w_1$. Also, $\text{tr}(W)$ is known since it is a function of $a, b, x$ and $y$, so $w_4$ is determined. Finally, $\text{det}(W)$ is similarly known, meaning that $w_2w_3 = w_1w_4-\text{det}(W)$ is also fixed. There are then $C\epsilon P^\epsilon$ choices for $w_2$ and $w_3$. All these terms together give the claimed bound.

For each such $W$, Lemma 5.3 bounds the number of choices $A$ from $H_{x,y}$ to $h$, which is at most $2^{k+1}$. Therefore, for each $k$, a maximum of $CP^{2+\epsilon}/x$ choices for $W$ and $A$ exist, where $A$ is in standard form with $a_1 = x$ and $a_4 = y$. Note that $k$ is bounded by $\log(P)$; then adding these terms up for all $k$ again yields $C\epsilon P^{2+\epsilon}/x$ total pairs, where the $\log(P)$ term has been absorbed into $P^\epsilon$.

Next, using Lemma 5.5 allows the restriction that $A$ be in standard form to be relaxed, at a cost of introducing a factor of $P^{2+\epsilon}/d$ to the prior estimate. Therefore, for a fixed value of $d$ with $d = xy$, there are a total of $C\epsilon P^{4+\epsilon}/(x^2y)$ possible choices for matrices $W$ and $A$. Adding these terms together over all choices for $x$ and $y$ with $xy = d \leq P^2$ gives a bound of $C\epsilon P^{4+\epsilon}$ as desired.

The one case remaining is the one where $\text{det}(A) = \text{det}(B) = 0$. However, since $\text{det}(A) = 0$ and $|A| \leq P$, $a_1$ and $a_4$ can be chosen freely amongst $P^2$ options; again choosing $a_2$ and $a_3$ amounts to selecting a factorization of a fixed number bounded by $P^2$, contributing $P^\epsilon$ to the estimate. Thus, $P^{2+\epsilon}$ choices for $A$ and for $B$ still yields a bound on the order of $P^{4+\epsilon}$. \textbf{QED}
5.3 Minor Arcs

With Theorem 5.6 comes a bound for $\int_{\Pi^2} |S_4(\alpha, \beta)| \, d\alpha d\beta$. There still remains the task of obtaining a uniform bound for $|S(\alpha, \beta)|$, which can then be used to complete the estimate for the minor arcs: $\int_{\Pi^2 - I_\theta} S_n(\alpha, \beta) \, d\alpha d\beta$.

Computing this quantity requires a much more thorough definition and analysis of the major arcs, which will vary with a parameter $\theta$ to be determined later. For now it is sufficient that $0 < \theta < 1$. Let $k, l, q$ be integers with $0 \leq k, l \leq q$ and define $I_\theta(k, l, q) = \{ (\alpha, \beta) \mid |\alpha - \frac{k}{q}| \leq \frac{1}{q} p^{-2+2\theta}, |\beta - \frac{l}{q}| \leq \frac{1}{q} p^{-2+2\theta} \}$, i.e. the set of points ‘close’ to the rational point $(\frac{k}{q}, \frac{l}{q})$. Then the major arcs $I_\theta$ are defined to be the set $\bigcup_{q \leq p^{2\theta}} \bigcup_{\gcd(k, l, q) = 1} I_\theta(k, l, q)$. Some fundamental properties of these sets are given in the next lemma.

**Lemma 5.7** Let $I_\theta(k, l, q)$ and $I_\theta$ be defined as above. Then

i) If $\theta < \frac{1}{2}$, $P > C_\theta$ and $(k, l, q) \neq (k', l', q')$, then $I_\theta(k, l, q) \cap I_\theta(k', l', q') = \varnothing$.

ii) $|I_\theta| \leq \sum_{q \leq p^{2\theta}} \sum_{\gcd(k, l, q) = 1} |I_\theta(k, l, q)| \leq p^{-4+6\theta}$.

iii) If $\theta \geq \frac{2}{3}$ then $I_\theta$ contains a fundamental domain of $\mathbb{R}^2/\mathbb{Z}^2$; that is $I_\theta = \Pi^2$.

**Proof:** For i), suppose $(\alpha, \beta) \in I_\theta(k, l, q) \cap I_\theta(k', l', q')$. Then by the triangle inequality, $|\frac{k}{q} - \frac{k'}{q'}| \leq |\alpha - \frac{k}{q}| + |\alpha - \frac{k'}{q'}| \leq (\frac{1}{q} + \frac{1}{q'}) P^{-2+2\theta}$. Since $\gcd(k, q) = \gcd(k', q') = 1$, $1 \leq |kq' - k'q|$ if $\frac{k}{q} \neq \frac{k'}{q'}$. But $|kq' - k'q| = qq'|k - k'| = qq' (\frac{1}{q} + \frac{1}{q'}) P^{-2+2\theta}$. Now $q \leq p^{2\theta}$ implies that $1 \leq 2P^{-2+4\theta}$. Since $\theta < \frac{1}{2}$, this gives a contradiction for $P$ sufficiently large. Finally, if $\frac{k}{q} = \frac{k'}{q'}$, then $\frac{1}{q} \neq \frac{1}{q'}$, and the argument applies to $\beta$ as well.

For ii), start by fixing a value of $q$. Then $|I_\theta(k, l, q)| = \frac{1}{q} P^{-4+4\theta}$, hence $\sum_{\gcd(k, l, q) = 1} |I_\theta(k, l, q)| \leq P^{-4+4\theta}$ since there are at most $q^2$ choices for $(k, l)$. Adding up this term over all $q \leq p^{2\theta}$ gives the desired result.

Finally for iii), let $(\alpha, \beta) \in \Pi^2$ and consider the collection of points $(q\alpha, q\beta) \mod 1$ for $1 \leq q \leq p^{2\theta}$. Divide $\Pi^2$ into $p^{2\theta}$ regular squares of size $P^{-\theta}$ by $P^{-\theta}$. Then
either there is a \((q\alpha, q\beta)\) in the block \([0, P^{-\theta}] \times [0, P^{-\theta}]\), or there are two points in the same block. In the latter case, let \(q_1\) and \(q_2\) be the associated values of \(q\). Then \(q' = |q_1 - q_2| \neq 0\) and \(|q'\alpha| = |q_1\alpha - q_2\alpha| \leq P^{-\theta}\), with the analogous result for \(q'\beta\).

Define \(||x||\) to be the distance from \(x\) to the nearest integer. Then by this argument, there exists a \(q\) such that \(||q\alpha||, ||q\beta|| \leq P^{-\theta}\). Choose \(k\) and \(l\) to be the integers close to \(q\alpha\) and \(q\beta\), respectively. Then \(|\alpha - k| \leq \frac{1}{q}P^{-\theta} \leq \frac{1}{q}P^{-2+2\theta}\), and similarly \(|\beta - l| \leq \frac{1}{q}P^{-2+2\theta}\). That is, \((\alpha, \beta) \in I_{\theta}\). QED

Now the main purpose of this section is to show that either there is a good bound on the value of \(|S(\alpha, \beta)|\), or \((\alpha, \beta) \in I_{\theta}\). This bound will be in terms of the cardinality of \(H_P\), a specialized set of lattice points. The next lemma lays the groundwork for this estimate.

**Lemma 5.8** For \(\alpha, \beta\) fixed, define \(H_P\) to be the set \(\{u, v \in \mathbb{Z} \text{ such that } |u| \leq 2P, |v| \leq 2P, ||2\alpha u + \beta v|| \leq 2/P, ||\beta u - 2(\alpha a + \beta b)v|| \leq 2/P\}\), where \(||x||\) denotes the distance from \(x\) to the nearest integer.

Then \(|S(\alpha, \beta)|^2 \leq P^2 \log^2(P)|H_P|\).

**Proof:** Write \(|S(\alpha, \beta)|^2\) as \(S(\alpha, \beta)\overline{S(\alpha, \beta)}\), which is a sum over \(x, y, x'\) and \(y'\). Write \(x' = x + u, y' = y + v\), and collect the \(x\) and \(y\) terms in the exponent. Taking absolute values, the summation may be extended over all \(u\) and \(v\) where \(|u|, |v| \leq 2P\).

This process is summarized by the equations

\[
|S(\alpha, \beta)|^2 = \sum_{u,v} \sum_{x,y} \exp(2\pi i[\alpha(b((x + u)^2 - x^2) - a((y + v)^2 - y^2))] \cdot \exp(2\pi i[\beta(b((x + u)(y + v) - xy) - e((y + v)^2 - y^2))] \cdot \chi \left( \frac{x}{P} \right) \chi \left( \frac{y}{P} \right) \chi \left( \frac{x + u}{P} \right) \chi \left( \frac{y + v}{P} \right) \leq \sum_{|u|, |v| \leq 2P} \left| \sum_{|x|, |y| \leq P} \exp(2\pi i[x(2\alpha u + \beta v) + y(\beta u - 2(\alpha a + \beta e)v)] \right|
\]

where \(\chi\) is a character of \(\mathbb{Z}/P\mathbb{Z}\).
The latter equation demonstrates how the conditions on $u$ and $v$ in $H_P$ arise. Now the inner sum is a product of two geometric series, both of the form

$$\left| \sum_{|x| \leq P} \exp(2\pi i \gamma x) \right| \leq \min \left( \sum_{|x| \leq P} 1, \left| \frac{\exp(2\pi i Px) - \exp(-2\pi i Px)}{1 - \exp(2\pi i \gamma)} \right| \right) \leq C \min(P, ||\gamma||^{-1}) \leq C' \frac{P}{1 + P||\gamma||}$$

Decompose the unit square $\Pi^2$ into $P^2$ regular squares $B_{k,l}$ with sides of length $P^{-1}$. Let $L_1(u, v) = 2\alpha bu + \beta bv$ and $L_2(u, v) = \beta bu - 2(\alpha a + \beta e)v$. Then define

$$N_{k,l} = \{(u, v) \in \mathbb{Z} \text{ such that } |u| \leq 2P, |v| \leq 2P, (\{L_1(u, v)\}, \{L_2(u, v)\}) \in B_{k,l}\},$$

where $\{x\}$ denotes the fractional part of $x$.

The goal is to show that $|N_{k,l}| \leq C|H_P|$. To do so, choose up to four representative entries $(u', v')$, one from each of the four quadrants in $\mathbb{Z}^2$. Any quadrant without points in $N_{k,l}$ is dropped without loss. Now, for every $(u, v)$ in the same quadrant as a particular $(u', v')$, it follows that $|u - u'|, |v - v'| \leq 2P$. Also, $|L_1(u - u', v - v')| = |L_1(u, v) - L_1(u', v')| \leq 1/P$, with a similar result holding for $L_2$. Thus, for each $(u, v)$ in the same quadrant as $(u', v')$, there corresponds the value $(u - u', v - v')$ which is an element of $H_P$. Therefore, $|N_{k,l}| \leq 4|H_P|$.

Then by rearranging the outer sum for $|S(\alpha, \beta)|^2$ to be indexed over the integer parts of $P||L_1(u, v)||$ and $P||L_2(u, v)||$ instead of $u$ and $v$ themselves, and bounding the inner sum with the geometric series computation above, yields

$$|S(\alpha, \beta)|^2 \leq C \sum_{|k|, |l| \leq P} \frac{P}{1 + |k|} \frac{P}{1 + |l|} |N_{k', l'}|$$

$$\leq C P^2 \sum_{|k|, |l| \leq P} \frac{1}{1 + |k|} \frac{1}{1 + |l|} |H_P|$$

$$\leq C P^2 \log^2(P) |H_P|$$

Note that $0 \leq k', l' < P, k' \equiv k \mod P$ and $l' \equiv l \mod P$. Also, the term for $k = l = 0$ appears twice, but its contribution is absorbed into $C$. QED
In order to convert this result into something applicable to points in $I_\theta$, $H_P$ must be generalized to a function depending on $\theta$. The next lemma from the geometry of numbers allows just that, requiring only that $H_P$ first be connected to a convex region in $\mathbb{R}^4$. This region $K_P$ is defined by $\{(u, v, s, t) \in \mathbb{R}^4 \text{ such that } |u|, |v| \leq 2P, |L_1(u, v) - s| \leq 2/P, |L_2(u, v) - t| \leq 2/P\}$. Then $H_P = K_P \cap \mathbb{Z}^4$ and the following applies.

**Lemma 5.9** Let $1 < L \leq P$ and let $K_{P,L} = L^{-1}K_P = \{(u, v, s, t) \in \mathbb{R}^4 \text{ such that } |u|, |v| \leq 2P/L, |L_1(u, v) - s| \leq 2/(PL), |L_2(u, v) - t| \leq 2/(PL)\}$. Then $|K_{P,L} \cap \mathbb{Z}^4| \geq CL^{-2}|K_P \cap \mathbb{Z}^4|$.

Using this lemma with $L = P^{1-\theta}$ gives a bound of $P^{4-2\theta} \log^2(P)|H_P(\theta)|$ for $|S(\alpha, \beta)|^2$, where $H_P(\theta) = \{(u, v) \in \mathbb{Z}^2 \text{ such that } |u|, |v| \leq 2P^\theta, ||L_1(u, v)|| \leq P^{-2+\theta}, ||L_2(u, v)|| \leq P^{-2+\theta}\}$.

Then everything is in place to prove the main theorem of this section, which shows that either $S(\alpha, \beta)$ is bounded by a nice function, or else $(\alpha, \beta)$ lies in a major arc.

**Theorem 5.10** Let $0 < \theta < 1$ and assume $(\alpha, \beta) \notin I_\theta$. Then for all positive $\epsilon$, $|S(\alpha, \beta)| \leq C_\epsilon P^{2-2\theta}$.

**Proof:** The idea will be to show that either $(\alpha, \beta) \in I_\theta$ or $H_P(\theta) = \{0\}$. So, assume $H_P(\theta) \neq \{0\}$, and take $(u, v)$ to be a nonzero element of this set.

Then by definition, $L_i(u, v) = m_i + t_i$, where $m_i \in \mathbb{Z}$ and $|t_i| \leq P^{-2+\theta}$. Then the aim is to solve these equations for $\alpha$ and $\beta$ using Cramer’s Rule. The denominator $q$ will be the determinant of the coefficient matrix $\begin{bmatrix} 2bu & bv \\ -2av & bu - 2ev \end{bmatrix}$, which is $2(bu - ev)^2 + 2(ab - e^2)v^2$, hence a positive integer. The numerator for $\alpha$ is then computed to be the determinant of the matrix $\begin{bmatrix} m_1 + t_1 & bv \\ m_2 + t_2 & bu - 2ev \end{bmatrix}$. This determinant may be broken up as the sum of the determinants of two matrices, one where the first column is reduced
to \([m_1, m_2]\), and another where it is reduced to \([t_1, t_2]\). Then if \(\alpha = k/q + \gamma/q\), where \(k\) is the determinant of the first matrix and \(\gamma\) is the determinant of the second, it only remains to show that \(|\gamma| \leq P^{2+2\theta}\) and \(q \leq P^{2\theta}\). However, these follow immediately from \(a, b\) and \(e\) being fixed, and \(|u|, |v| \leq P\).

Finally, if \(|H_P(\theta)| = 1\), the result follows from Lemma 5.8. QED

Therefore, the contribution of the minor arcs to the value of \(N_P\) is

\[
\int \int_{\Pi^2-I_0} S_n(a, \beta) \, d\alpha d\beta \leq \int \int_{\Pi^2-I_0} |S(a, \beta)|^4 |S(a, \beta)|^{n-4} \, d\alpha d\beta \leq CP^{(2-2\theta)(n-4)} \int \int_{\Pi^2} |S(a, \beta)|^4 \, d\alpha d\beta \leq CP^{2n-8-2\theta(n-4)+4+\epsilon}
\]

### 5.4 Major Arcs

The next step in the process is to determine the contribution of the major arcs to \(N_P\). The advantage of being in a major arc is that the values for \(\alpha\) and \(\beta\) are very close to rational numbers, hence the exponential sums should be essentially periodic. At the cost of an error term, the nonperiodic portion of the sum will be split off and estimated by an integral.

Therefore, choose a \((k, l, q)\) arc to evaluate \(S_n(a, \beta)\) on. Then \(\alpha = k/q + \delta\) and \(\beta = l/q + \gamma\), where \(|\delta|, |\gamma| \leq P^{2+2\theta}/q\). Denote by \(S_n(a, \beta; k, l, q)\) the restriction of \(S_n(a, \beta)\) to this block. Then

\[
S_n(a, \beta; k, l, q) = \sum_{X, Y, S, T \in \mathbb{Z}^n} \exp \left( 2\pi i \left( (\delta + \frac{k}{q})(b(qX + S)^2 - a(qY + T)^2) \right) \right) \cdot \exp \left( 2\pi i \left( (\gamma + \frac{l}{q})(b(qX + S)(qY + T) - c(qY + T)^2) \right) \right) \cdot \chi \left( \frac{qX + S}{P} \right) \chi \left( \frac{qY + T}{P} \right)
\]

where \(0 \leq s_i, t_i < q\) for \(1 \leq i \leq n\). It is clear that the value for the sum when \(\delta, \gamma = 0\) depends only on \(S\) and \(T\), since the \(X\) and \(Y\) components shift the argument by
integral multiples of $2\pi$. Therefore, split up the exponential function into the product of two terms, one containing $\frac{k}{q}$ and $\frac{l}{q}$, and the other containing $\delta$ and $\gamma$. Then the latter summation can be pulled out of the portion depending on $X$ and $Y$, yielding

$$\sum_{S, T \mod q} \exp \left( 2\pi i \frac{kbS^2 + lbRS - (ka + le)T^2}{q} \right) G(S, T)$$

where $G(S, T)$ is the remaining inner sum,

$$G(S, T) = \sum_{X, Y} \exp \left( 2\pi i \left[ \delta(b(qX + S)^2 - a(qY + T)^2) \right] \right) \cdot \exp \left( 2\pi i \left[ \gamma(b(qX + S)(qY + T) - e(qY + T)^2) \right] \right) \cdot \chi \left( \frac{qX + S}{P} \right) \chi \left( \frac{qY + T}{P} \right)$$

Define $\phi_{\alpha, \beta}(qX + S, qY + T)$ to be the exponent on $\exp(2\pi i)$ in $G(S, T)$. The idea will be to estimate the sum with the corresponding integral, therefore the error incurred by this change must be estimated. To do this, fix a choice for $X$ and $Y$, and compare that term in the sum to the integral over the corresponding block $(\Pi^\alpha + X, \Pi^\alpha + Y)$. In the following arguments, $X'$ and $Y'$ shall denote the variables of integration, both in $\Pi^\alpha$.

The first observation to make is that changing the characteristic function from $\chi \left( \frac{q(X + X') + S}{P} \right) \chi \left( \frac{q(Y + Y') + T}{P} \right)$ to $\chi \left( \frac{qX + S}{P} \right) \chi \left( \frac{qY + T}{P} \right)$ has no effect except for the boundry terms where $||X|| = P$ or $||Y|| = P$. There are on the order of $(P/q)^{2n-1}$ such terms, each of magnitude at most 1. Integrating this bound over all of the major arcs yields a total error of size $(P/q)^{2n-1} P^{-4+6t} < P^{2n-5+6t}$.

The other change to make is to the exponential function. The form to be used here is that

$$\left| \int \exp(2\pi ix) - \exp(2\pi i t) \right| \leq \int |\exp(2\pi i(x - t)) - 1| \cdot |\exp(2\pi i t)| \leq \int 2\pi |x - t|$$

Then it is sufficient to estimate $|\phi_{\alpha, \beta}(q(X + X') + S, q(Y + Y') + T) - \phi_{\alpha, \beta}(qX + S, qY + T)|$. Computing this term explicitly, then using the facts that $a, b$ and $e$
are fixed constants, $|X|, |Y| \leq CP$, $|S|, |T| \leq Cq$ and $|X'|, |Y'| \leq C$, a bound of $C'(|\alpha| + |\beta|)q^2P$ may be achieved. Now, $|\alpha|, |\beta| \leq P^{-2+2\theta}/q$ and $q \leq P^{2\theta}$ simplify this even further to a term on the order of $P^{-1+4\theta}$. Finally, as before, summing over all $(P/q)^{2n}$ blocks and integrating over $I_\theta$ yields an error bound on the order of $P^{2n-5+10\theta}$.

Therefore, make the change from estimating $G(S, T)$ to evaluating the integral

$$\int_{X,Y} \exp(2\pi i \phi_{\alpha, \beta}(qX+S, qY+T)) \chi \left( \frac{qX+S}{P} \right) \chi \left( \frac{qY+T}{P} \right) dX dY.$$  

Then, perform a change of variables $X' = qX + S$, $Y' = qY + T$. This simplifies the integrand greatly, and introduces a factor of $q^{-2n}$ which comes out of the integral. This has the further benefit of completely removing any dependence on $S, T$ from the estimate for $G(S, T)$.

Hence, on shifting the $q^{-2n}$ term to the summation, the problem has been reduced to

$$|S_n(\alpha, \beta; k, l, q)| \leq |K_n(k, l, q)| \cdot |L(\delta, \gamma; k, l, q)| + E(\theta)$$

where the various terms are defined as

$$K_n(k, l, q) = \frac{1}{q^n} \sum_{S, T \text{ mod } q} \exp \left( 2\pi i \frac{kbS^2 + lbST - (ka + le)T^2}{q} \right)$$

$$L(\delta, \gamma; k, l, q) = \int_{X,Y} \exp \left( 2\pi i \phi(X, Y) \right) \chi \left( \frac{X}{P} \right) \chi \left( \frac{Y}{P} \right)$$

$$|E(\theta)| \leq P^{2n-5+10\theta}$$

The next two sections will focus on $K(k, l, q)$ and $L(\delta, \gamma; k, l, q)$ respectively.

### 5.5 Exponential Sum Estimates

Write $K(k, l, q)$ for $K_1(k, l, q)$; then as was the case for $S_n(\alpha, \beta)$, it follows that $K_n(k, l, q) = K(k, l, q)^n$. Now define $K_n(q) = \sum_{\gcd(k, l, q)=1} K(k, l, q)^n$; it will be shown in this section that $K(q)$ has nice multiplicative properties, which may be used to evaluate it in terms of ‘local densities of solutions’.
The first couple of lemmas are designed to establish a good bound on the size of \(K_n(q)\) by first limiting the size of \(K(k, l, q)\), and then limiting the number of terms in the sum for \(K_n(q)\).

**Lemma 5.11** Let \(\gcd(k, l, q) = 1\). Then \(|K(k, l, q)|^2 \leq Cq^{-2}D\), where \(D\) is defined to be \(\gcd(q, \Delta(k, l))\), where in turn \(\Delta(k, l) = |\det\left[\frac{2bk}{bl - 2(kx + le)}\right]|\).

**Proof:** Begin by writing \(|K(k, l, q)|^2\) as \(K(k, l, q)K(k, l, \overline{q})\). This yields a sum over \(x, y, x', y'\)

\[
\frac{1}{q^4} \sum_{x, y, x', y' \mod q} \exp\left(\frac{2\pi i}{q} [k(b(x'^2 - x^2) - a(y'^2 - y^2)) + l(b(x'y' - xy) - e(y'^2 - y^2))]\right)
\]

Now writing \(x' = x + u\) and \(y' = y + u\) reduces the term to

\[
\frac{1}{q^4} \sum_{x, y, u, v \mod q} \exp\left(\frac{2\pi i}{q} [k(b(2xu + u^2) - a(2yv + v^2))]\right) \cdot \exp\left(\frac{2\pi i}{q} [l(b(xv + uy + uv) - e(2yv + v^2))]\right)
\]

Next, move the terms which depend only on \(u\) and \(v\) outside the summation over \(x\) and \(y\).

\[
\frac{1}{q^4} \sum_{u, v \mod q} \exp\left(\frac{2\pi i}{q} (kbu^2 - kav^2 + lbuv - lev^2)\right) \cdot \sum_{x, y \mod q} \exp\left(\frac{2\pi i}{q} (2kbu + lbv + y(lbu - 2av - 2ev))\right)
\]

Finally, this term can be approximated by taking absolute values over the \(u, v\) summation, eliminating the outer exponential term.

\[
\frac{1}{q^4} \sum_{u, v \mod q} \left| \sum_{x, y \mod q} \exp\left(\frac{2\pi i}{q} x f(u, v) + yg(u, v)\right)\right|
\]

Now for each \((u, v)\) pair where \(f(u, v) \equiv g(u, v) \equiv 0 \mod q\), this inner sum evaluates to \(q^2\) 1’s. However, if without loss of generality \(f(u, v) \not\equiv 0 \mod q\), then taking the inner sum over the values of \(x\) yields a full set of \(q\)th roots of unity,
making the term equal to 0. Therefore, an upper bound for $|K(k, l, q)|^2$ is given by $q^{-2} \cdot |\{(u, v) \text{ such that } f(u, v) \equiv g(u, v) \equiv 0 \mod q\}|$, where $f(u, v) = 2kbu + lbv$ and $g(u, v) = lbv - (2a + 2e)v$.

This then gives two linear equations in $u$ and $v$, and solving them simultaneously yields the conditions $\Delta(k, l)u \equiv \Delta(k, l)v \equiv 0 \mod q$. The intention is to continue reducing common factors out of these equations until a nontrivial restriction on $u$ and $v$ arises. To start, take $D = \gcd(q, \Delta(k, l))$, and clear this factor out of both equations. This leaves $\Delta' u \equiv \Delta' v \equiv 0 \mod q'$, where $\Delta' = \Delta(k, l)/D$ and $q' = q/D$.

Suppose $u'$ is chosen freely. Then $u' = u/q' \leq q/q' = D$ has at most $D$ options. Now $v'$ is fixed mod $D/g$, and similarly $v' \leq D$, so there are at most $g$ choices for $v'$. Having chosen $u'$ and $v'$ immediately determines $u$ and $v$, so there are at most $gD \leq 2bD = CD$ values for $(u, v)$, which proves the lemma. QED

Since a bound for $K(k, l, q)$ has been established in terms of $D$, a restriction on how many choices for $k$ and $l$ give rise to a particular $D$ will be important. The following lemma provides exactly that.

**Lemma 5.12** Let $D$ be a factor of $q$. Then for all $\epsilon > 0$, there are at most $C_\epsilon q^{2+\epsilon}/D$ values for $k$ and $l$ where $0 \leq k, l < q$, $\gcd(k, l, q) = 1$ and $\gcd(\Delta(k, l), q) = D$.

**Proof:** Consider first the weaker conditions that $0 \leq k', l' < D$, $\gcd(k', l', D) = 1$ and $\Delta(k', l') \equiv 0 \mod D$. 
Note that $-\Delta(k', l')$ may be expressed in the nice form $4(ab - e^2)k'^2 + (bl' + 2ek)l^2$. Also, $\gcd(k', bl' + 2ek', D) = \gcd(k', bl', D) | \gcd(bl', bl', bD) = b \gcd(k', l', D) = b$, hence the gcd of these three terms is bounded by a constant.

Perform the change of variables $k'' = k', l'' = bl' + 2ek'$; then solving for $k''$ and $l''$ gives a bounded number of solutions for $k'$ and $l'$. The expression for $\Delta(k', l')$ now translates to solving $4(ab - e^2)k'^2 + l'^2 \equiv 0 \mod D$. Now, use the fact that the number of solutions to this equation when $\gcd(k'', l'', D) = 1$ is bounded by $C_1D^{1+\epsilon}$. Heuristically, $k''$ can be chosen freely, resulting in computing $l''$ as a square root mod $D$. This in turn gives $2^{\omega(D)} \approx 2^{\log \log(D)} < D^\epsilon$ choices for $l''$, where $\omega(D)$ is the number of distinct prime factors of $D$.

Finally, selecting $k$ and $l$ congruent to $k'$ and $l'$ mod $D$ introduces a factor of $(q/D)^2$ choices, proving the lemma. QED

The following lemma combines the prior results in order to provide a strong bound on the size of $|S_n(q)|$.

**Lemma 5.13** For all $\epsilon > 0$, $|S_n(q)| \leq C_4 q^{-\frac{3}{2}+\epsilon}$.

Immediate consequences of this lemma are that the series $\sum_{1 \leq q < \infty} S_n(q)$ is absolutely convergent, and the tail $\sum_{q \geq p_2^\theta} |S_n(q)|$ is bounded by $P^{-\theta+\epsilon}$.

**Proof:** From Lemmas 5.11 and 5.12 directly follow

$$|K(q)| \leq C \sum_{D|q} q^{-n} D^{n/2} \left| \{k, l \text{ s.t. } \gcd(k, l, q) = 1, \gcd(q, \Delta(k, l)) = D \} \right|$$

$$\leq C q^{-n+2+\epsilon} \sum_{D|q} D^{n/2-1} \leq C q^{-n+2+\epsilon} q^{n/2-1} q^\epsilon$$

where it has been used that there are $q^\epsilon$ divisors of $q$. Then noting that $n \geq 5$ finishes the result. QED

The next goal is to prove that the $K(k, l, q)$ obey some fundamental multiplicative properties.
Lemma 5.14 Let \( q = q_1 q_2 \), with \( \gcd(q_1, q_2) = 1 \). Then \( K(k, l, q) = K(q_2 k, q_2 l, q_1) K(q_1, q_1 l, q_2) \).

Proof: This argument is essentially the Chinese Remainder Theorem. That is, for \( s \in (\mathbb{Z}/q) \), there exists a unique point \((s_1, s_2)\) in \((\mathbb{Z}/q_1) \times (\mathbb{Z}/q_2)\) such that \( s/q \equiv s_1/q_1 + s_2/q_2 \mod 1 \). Also, \( s^2/q = q(s/q)^2 \equiv q_2 s_1^2/q_1 + q_1 s_2^2/q_2 \mod 1 \). Let \( t, t_1 \) and \( t_2 \) hold a similar relationship.

These equations are used when combining a pair of terms from \( K(q_2 k, q_2 l, q_1) \) and \( K(q_1 k, q_1 l, q_2) \):

\[
\exp \left( \frac{2\pi i}{q_1} [q_2 k (bs_1^2 - at_1^2) + q_2 l (bs_1 t_1 - ct_1^2)] \right),
\exp \left( \frac{2\pi i}{q_2} [q_1 k (bs_2^2 - at_2^2) + q_1 l (bs_2 t_2 - ct_2^2)] \right)
= \exp \left( \frac{2\pi i}{q} [k (bs^2 - at^2) + l (bst - ct^2)] \right)
\]

This then results in a general term from \( K(k, l, q) \), and the CRT guarantees that the terms are in a one-to-one correspondence with each other. QED

Lemma 5.15 \( K_n(q) \) is a multiplicative function; that is, if \( \gcd(q_1, q_2) = 1 \), then \( K_n(q_1 q_2) = K_n(q_1) K_n(q_2) \).

Proof: Let \( q = q_1 q_2 \). Again by the Chinese Remainder Theorem, it is sufficient to show that there is a bijection between points \((k, l)\) in \((\mathbb{Z}/q)^2\) and pairs of points \([(q_2 k, q_2 l), (q_1 k, q_1 l)]\) in \((\mathbb{Z}/q_1)^2 \times (\mathbb{Z}/q_2)^2\), where \((\mathbb{Z}/q)^2\) denotes points \((k, l)\) with \( \gcd(k, l, q) = 1 \).

Suppose \( \gcd(k, l, q) = 1 \), but \( p | \gcd(q_2 k, q_2 l, q_1) \), where \( p \) is a prime. Then \( p | q_1 \mid q \), but \( p \) can not divide all three of \( k, l \) and \( q \), therefore it either does not divide \( k \) or \( l \). In either case, \( p \) divides \( q_2 k \) and \( q_2 l \), so \( p \) divides \( q_2 \). But \( \gcd(q_1, q_2) = 1 \), giving a contradiction. Therefore, a mapping between the two sets exists and is well defined.

It remains to show that for every pair of points \([(k_1, l_1), (k_2, l_2)]\) in the image space, there exists a unique point \((k, l)\) corresponding to it in the domain. This
forms the system of equations $q_2k \equiv k_1 \mod q_1, q_2l \equiv l_1 \mod q_1, q_1k \equiv k_2 \mod q_2$
and $q_1l \equiv l_2 \mod q_2$. Since $q_1$ and $q_2$ are relatively prime, they are invertible in $(\mathbb{Z}/q_2)$ and $(\mathbb{Z}/q_1)$ respectively, hence the system of equations gives congruences for $k$ and $l$ mod $q_1$ and $q_2$. The CRT then gives a unique solution mod $q$. QED

Therefore, $\sum_{1 \leq q < \infty} K_n(q)$ is a convergent series, and by the property of multiplicative functions may be evaluated as $\prod_p \sum_{0 \leq r < \infty} K_n(p^r)$, where the product is over the set of primes. The final step is to estimate this inner sum.

**Lemma 5.16** The above inner sum is the asymptotic density of $p$-adic solutions. In particular, $\sum_{0 \leq r \leq R} K_n(p^r) = N(p^R)p^{-R(2n-2)}$, where $N(p^r) = |\{(S, T) \in (\mathbb{Z}/p^r)^2 \text{ such that } bS^2 - aT^2 \equiv bST - eT^2 \equiv 0 \mod p^r\}|$.

**Proof:** The proof proceeds by showing that the sum telescopes. First, expand the summation in terms of the $K_n(k, l, q)$s.

$$\sum_{0 \leq r \leq R} K_n(p^r) = \sum_{0 \leq r \leq R} \sum_{\gcd(k, l, p) = 1} K(k, l, p^r)$$

Next, expand out $K(k, l, p^r)$, and move the $p^{-2rn}$ term out of the inner sums.

$$\sum_{0 \leq r \leq R} \frac{1}{p^{2rn}} \sum_{\gcd(k, l, p) = 1} \sum_{S, T \in (\mathbb{Z}/p^r)^n} \exp \left(\frac{2\pi i}{p^r}(kf(S, T) + lg(S, T))\right)$$

Notice that summing over $0 \leq k, l < p^r, \gcd(k, l, p) = 1$ is the same as summing over $0 \leq k, l < p^r$, and then subtracting off the terms in that sum where $p \mid k, l$. Therefore, switch the order of summations between $S, T$ and $k, l$.

First consider the sum over all $k$ and $l$. As in earlier proofs, this sum depends on whether or not $f(S, T) \equiv g(S, T) \equiv 0 \mod p^r$. If they are, then the inner sum contributes $p^{2r}$, otherwise 0. Summing this function over all $S$ and $T$ yields $p^{2r}N(p^r)$, which when multiplied by the leading $p^{-2rn}$ becomes $p^{-2r(n-1)}$.

Now consider the negated sum over $p \mid k, l$. With $p$ dividing the exponent, the requirements on $f$ and $g$ are relaxed to $f(S, T) \equiv g(S, T) \equiv 0 \mod p^{-1}$. If
these are passed, then a total of \( p^{2r-2} \) is contributed to the sum since \( k \) and \( l \) can range over \( p^{r-1} \) choices each. Again, if the conditions fail, 0 is contributed instead. Since \( S \) and \( T \) take values in \( (\mathbb{Z}/p^r)^n \), every solution for \( f \) and \( g \) mod \( p^{r-1} \) gives rise to \( p^{2n} \) solutions mod \( p^r \). Combining these factors gives a total contribution of

\[
p^{-2r-2} p^{2n} N(p^{r-1}) = p^{-2(r-1)(n-1)} N(p^{r-1}),
\]

which is exactly the \( r-1 \) term in the other sum.

Then the sum is indeed telescoping.

\[
\sum_{0 \leq r \leq R} (N(p^r)p^{-2r(n-1)} - N(p^{r-1})p^{-2(r-1)(n-1)}) = N(p^R)p^{-2R(n-1)}
\]

QED

Taking \( A_n(p) = \lim_{r \to \infty} N(p^r)p^{-2r(n-1)} \), the local density of solutions, the exponential sum may be expressed in the form

\[
\sum_{1 \leq q < \infty} K_n(q) = \prod_p A_n(p)
\]

5.6 Evaluating the Singular Integral

The last task is to evaluate the singular integral \( L(\delta, \gamma; k, l, q) \). The first thing that must be accomplished is extending the integral from the major arcs to all of \( \mathbb{R}^2 \); this allows it to be completely separated from the exponential sum. The other goal is to show that the integral is positive, and thus that the expected final term is larger than the errors gathered during this process.

The first lemma gives a good bound for \( L(\delta, \gamma) \), which will be used to show that integrating the function away from the major arcs does not contribute more than an error term.

**Lemma 5.17** Let \( L(\delta, \gamma) \) equal

\[
\int_{\mathbb{R}^2} \exp \left( 2\pi i [\delta(bx^2 - ay^2) + \gamma(bxy - ey^2)] \right) \chi(x/P) \chi(y/P) \, dx \, dy
\]

Then \( |L(\delta, \gamma)| \leq CP^{2+\varepsilon}(1 + P^2(|\delta| + |\gamma|))^{-1} \).
Proof: Perform a change of variables, \( x' = x/P \) and \( y' = y/P \). Then follow the procedure used in the exponential sum estimates; compute \( |L(\delta, \gamma)|^2 \) as \( L(\delta, \gamma)\overline{L(\delta, \gamma)} \). This gives an integration over four variables, call them \( x, y, x' \) and \( y' \). Replace \( x' \) with \( x + u \) and \( y' \) with \( y + v \). Then \(|u|, |v|\) are bounded by 2 since the characteristic function eliminates any values of \( x, y, x' \) or \( y' \) with size greater than 1 from the integral.

At this point, the terms that depend only on \( u \) and \( v \) may be pulled out of the inner integral in \( x \) and \( y \), and absolute values taken. Therefore, the estimate is in the form

\[
P^4 \int_{|u|, |v| \leq 2} \left| \int_{\mathbb{R}^2} \exp\left(2\pi i P^2 [x(2b\delta u + b\gamma v) + y(b\gamma u - 2(a\delta + e\gamma)v)]\right) \chi(x, y) \right|
\]

Now substitute \( u' \) for \( 2b\delta u + b\gamma v \) and \( v' \) for \( b\gamma u - 2(a\delta + e\gamma)v \). Then the inner integrand is \( \exp(2\pi i P^2 (xu' + yv'))\chi(x)\chi(y) \), where \( u' \) and \( v' \) are independent of \( x \) and \( y \). Hence the integral may be decomposed into two separate integrals of the form \( \int_{\mathbb{R}} \exp(2\pi itx)\chi(x)dx \). With the characteristic function, this becomes an integral from -1 to 1.

Then, taking the trivial bound on a complex exponential function gives an upper limit of 2 for the value of this subintegral. Alternatively, carrying out the integration yields \((2\pi it)^{-1}(\exp(2\pi it) - \exp(-2\pi it))\), which also is trivially bounded by \( C/t \). Therefore, \( \left| \int_{\mathbb{R}} \exp(2\pi itx)\chi(x)dx \right| \leq C \min(1, 1/|t|) \leq C(1 + |t|)^{-1} \).

Taking \( t = P^2 u' \) for the \( x \) integral and \( t = P^2 v' \) for the \( y \) integral gives

\[
\left| \int_{\mathbb{R}^2} \exp(2\pi i P^2 (xu' + yv'))\chi(x)\chi(y)dydx \right| \leq C(1 + P^2 |u'|)^{-1}(1 + P^2 |v'|)^{-1}.
\]

Just as in the proof of Lemma 5.8, decompose \( \Pi^2 \) into \( 4P^4 \) regular blocks \( B_{i,j} \), each of side length \( P^{-2}/2 \). The purpose here is to estimate how many values of \( (u', v') \) land in a block \( B_{i,j} \). Note that \(|u'| = |2b\delta u + b\gamma v| \leq 2b|\delta||u| + b|\gamma||v| \leq 6b\), with a similar result for \( v' \); thus \(|u'|, |v'| \) are less than a fixed constant. In turn, this
means that restricting to values of \((u', v') \in \Pi^2\) only scales the following argument by a constant factor.

Now, if the set \(N_{i,j} = \{(u, v) \text{ such that } (u', v') \in B_{i,j}\}\) is nonempty, choose a representative element \((u_1, v_1)\) from it. Then for all \((u_2, v_2) \in N_{i,j}\), it follows that \((u_1 - u_2, v_1 - v_2) \in N\) where \(N = \{(u, v) \text{ such that } |u'|, |v'| \leq 1/P^2\}\). Therefore, \(\text{meas}(N_{i,j}) \leq \text{meas}(N)\) for all \(i\) and \(j\). This then implies

\[
|L(\delta, \gamma)|^2 \leq C \sum_{0 \leq s \leq P^2} \sum_{0 \leq t \leq P^2} \frac{1}{1 + P^2s} \frac{1}{1 + P^4t} \sigma(N) \leq CP^4 \log^2(P) \sigma(N)
\]

where \(\sigma(N) = \text{meas}(N)\). It just remains to estimate \(\sigma(N)\). To do so, note that \(|u'| = |2b\delta u + b\gamma v| \geq C \max(|\delta u|, |\gamma v|)\), and similarly \(|v'| \geq C' \max(|\gamma u|, |\delta v|)\). Therefore, \(|u'| + |v'| \geq C''|\delta + \gamma| \max(|u|, |v|)\). Now, knowing the maximum value of a coordinate gives an upper bound on the norm of a point; similarly, knowing the minimum value of the sum of the two coordinates gives a lower bound on the norm of a point. Then the last inequality implies that \(|(u', v')| \geq C(|\delta| + |\gamma|)(u, v)|\).

Using this relationship between norms of \((u, v)\) and \((u', v')\), the estimate for \(\sigma(N)\) follows:

\[
\sigma(\{(u, v) \text{ s.t. } |u'|, |v'| \leq P^{-2}\}) \leq C \sigma(\{(u, v) \text{ s.t. } |(u, v)| \leq \frac{1}{P^2(|\delta| + |\gamma|)}\}) \\
\leq C' \frac{1}{P^4(|\delta| + |\gamma|)^2}
\]

Finally, this implies that \(|L(\delta, \gamma)|^2 \leq P^4 \log^2(P)(P^4(|\delta| + |\gamma|)^2)^{-1}\). Combined with the trivial estimate that \(|L(\delta, \gamma)|^2 \leq P^4\), this gives the desired result. QED

An immediate corollary of this proof is that \(\int_{|\delta| + |\gamma| \geq P^{-2+2n/q}} |L(\delta, \gamma)|^n d\delta d\gamma\) is bounded by \(P^{2n-4+\epsilon}(P^{2g}/q)^{2-n}\). This follows from using the nontrivial bound for \(|L(\delta, \gamma)|^2\) from the last proof and using standard integration techniques. Then, the integral may be extended to all of \(\mathbb{R}^2\) with a known error term, eliminating any dependency on \(\delta\) or \(\gamma\).
So, define \( L_P \) to be
\[
P^{2n} \int_{\mathbb{R}^2} \int_{\mathbb{R}^{2n}} \exp\left(2\pi i P^2[\alpha(bX^2 - aY^2) + \beta(bXY - eY^2)]\right) \chi(X, Y) \, dX \, dY \, d\alpha \, d\beta
\]

This then is the singular integral. It just remains to show that it is positive, so that the main term in the estimate for the number of solutions is nondegenerate. To begin, perform a change of variables from \( P^2 \alpha \) and \( P^2 \beta \) to \( \alpha \) and \( \beta \). This removes any dependency on \( P \) inside the integral, by bringing a \( P^{-4} \) outside. Then \( L_P = P^{2n-4} L_1 = P^{2n-4} L \).

The integral is unaffected by the removal of a single point, so remove the origin from \( \mathbb{R}^{2n} \); then there is always a coordinate \( x_i \) or \( y_i \) which is nonzero. Assume without loss that this coordinate is \( x_1 \). Then the map \( \phi \) which maps \( \mathbb{R}^{2n} \) to \( \mathbb{R}^2 \) by \( \phi(X, Y) = (bX^2 - aY^2, bXY - eY^2) \) is well defined. This is clear because \( \phi' = \begin{bmatrix} 2bx_1 & -2ay_1 \\ by_1 & bx_1 - 2ey_1 \end{bmatrix} \) has the minor \( \begin{bmatrix} 2bx_1 & -2ay_1 \\ by_1 & bx_1 - 2ey_1 \end{bmatrix} \), which has a nonzero determinant. That is, \( \phi' \) has full rank.

Extend \( \phi \) to a function from \( \mathbb{R}^{2n} \) to \( \mathbb{R}^{2n} \) by taking \( \phi(U, V) = (u_1, u_2, \ldots u_n) = (u_1, U') \), with similar notation for \( V \). Also, let \( \rho(U, V) = \rho(u_1, U', v_1, V') = J(U, V) \chi(\phi^{-1}(U, V)) \). Since \( \rho \) is a Jacobian multiplied by a characteristic function, it is always nonnegative. In fact, \( \rho(0, U', 0, V') \) represents the surface in \( \mathbb{R}^{2n} \) which satisfies the equations \( bX^2 - aY^2 = 0, bXY - eY^2 = 0 \), which has been weighted by the Jacobian factor. Since this surface arises from rational scalings of triangles, it is nonempty, and thus \( \rho(0, U, 0, V) \) is positive on some open set.
This fact finishes the argument, since applying the Fourier Transform and Fourier Inversion Formula gives

\[
L = \int_{\mathbb{R}^2} \int_{\mathbb{R}^{2n}/\{0\}} \exp(2\pi i (\alpha u_1 + \beta v_1)) \rho(u_1, U', v_1, V') dU dV d\alpha d\beta
\]

\[
= \int_{\mathbb{R}^{2n-2}} \int_{\mathbb{R}^2} \hat{\rho}(\alpha, U', \beta, V') d\alpha d\beta dU' dV'
\]

\[
= \int_{\mathbb{R}^{2n-2}} \rho(0, U', 0, V' dU') dV'
\]

And thus, \( L > 0 \).

Therefore, the number of representations of a rational scaling of a triangle may be computed as the integral of an exponential sum, where the exponent contains a representative pair of homogeneous equations. By dividing the unit square into major and minor arcs, the integral may be decomposed into pieces. The minor arcs contribute only an error term. The major arcs are based around rational points where the exponential sum is relatively stable. By accepting more error terms, the sum may be decomposed into a nicer version with multiplicative properties, along with a new integral.

The new integral may be extended beyond the major arcs at the cost of another error term; then it is rendered independent of the summation and may be computed directly as a measure of a surface associated to the set of triangles under study. Finally, the sum may be decomposed by prime factors, and shown to contribute measurements on the \( p \)-adic densities of solutions.

Putting all of these results together gives

**Theorem 5.18** Let \( N_P \) denote the number of embeddings of rational scalings of a triangle characterized by \((a, b, c)\), under the restriction that the sides \(X, Y\) satisfy \(||X||, ||Y|| \leq P\). Then

\[
N_P = P^{2n-4} \rho \prod_p A_p + E_P
\]
where $\rho$ is the measure of a surface based on the triangle, $A_p$ is the density of $p$-adic solutions to the embedding problem, and $E_P$ is an error term bounded by $P_{2n-4-1/4}$. 
Chapter 6

Higher Dimensional Simplices

The natural extension of this dissertation is to the question of embedding higher dimensional simplices into $\mathbb{Z}^n$. Prior work by Kitoaka suggests that a $k$ dimensional simplex may be embedded into a $2k + 3$ dimensional space. But Lagrange has shown that a one dimensional simplex may be embedded in four dimensions, and Theorem 4.4 states that a two dimensional simplex may be embedded in five. Thus, it is not unreasonable to expect that a refinement of Kitoaka’s general result may be possible.

6.1 Necesssary Conditions

Establishing the necessary conditions for a simplex to even have a possibility of being embedded into an integer lattice is best done by considering the matrix form of the associated equations. Let $k$ be the dimension of the simplex in question, and suppose $0, X_1, X_2, \ldots X_k$ are lattice points in $\mathbb{Z}^n$ which given an embedding. Let $A$ be the matrix whose columns are the vectors $X_i$, and let $B = A^t A$. Then $B$ is the Gram Matrix corresponding to the simplex; since $A$ is an integral $n$ by $k$ matrix, it follows that $B$ is an integral, symmetric $k$ by $k$ matrix.

In order for $B$ to be a Gram Matrix, it is necessary and sufficient that it be positive definite, or equivalently, that all $k$ upper left minors of $B$ have a positive determinant. This gives an easy-to-check list of equations.
Thus, assuming that $B$ is the Gram Matrix of a simplex, write $B = [b_{ij}]$ and consider the system of $k(k + 1)/2$ equations:

$$X_i^tX_j = b_{ij}, 1 \leq i \leq j \leq k$$  \hspace{1cm} (6.1)

Since there trivially is a solution to these equations over $\mathbb{R}$ for $n \geq k$, the question is when there are solutions over $\mathbb{Z}_p$. In addition, if $\rho_p$ (the density of $p$-adic solutions) can be shown to be sufficiently large, then heuristically there should be actual integer solutions as well.

### 6.2 Preliminary Estimates

To obtain a large number of $p$-adic solutions for large primes $p$, a more analytic approach to solving Equations 6.1 will be used. This requires finding linearly independent solutions to the equations, mod $p$, which may then be lifted to many solutions in $(\mathbb{Z}/p^r)$ using Hensel’s Lemma. Note that for this chapter, $(\mathbb{Z}/p)$ shall denote the integers mod $p$ and $(\mathbb{Z}/p)^{nk}$ shall be the set of $n$ by $k$ matrices over $(\mathbb{Z}/p)$.

Due to the quadratic nature of this problem, it is only natural to expect that a Gaussian Sum shall become involved; the primary form used in the proofs is evaluated in the following lemma.

**Lemma 6.1** Let $S$ be a symmetric, $k$ by $k$ matrix over $\mathbb{Z}/p$. Define $G(S) = \sum_{X \in (\mathbb{Z}/p)^{nk}} \exp(\frac{2\pi i}{p} tr(SX^tX))$, where $\exp(x)$ is the standard exponential function $e^x$ and $tr(A)$ is the trace of the matrix $A$. Then, taking $r$ to be the rank of $S$, $|G(S)| \leq p^{nk-nr}$.

**Proof:** Using the facts that matrix multiplication and the trace operator are linear functions, and that $G(S) \overline{G(S)} = |G(S)|^2$, it follows that

$$|G(S)|^2 = \sum_{X,Y \in (\mathbb{Z}/p)^{nk}} \exp \left( \frac{2\pi i}{p} tr(S(X^tX - Y^tY)) \right)$$
Let \( U = X - Y \). Then \( X^tX - Y^tY = (Y + U)^t(Y + U) - Y^tY = Y^tU + U^tY + U^tU \). Substituting this in to the last equation and splitting up the summation yields

\[
\sum_{U \in \mathbb{Z}/p} \left( \exp \left( \frac{2\pi i}{p} \text{tr}(SU^tU) \right) \sum_{Y \in \mathbb{Z}/p} \exp \left( \frac{2\pi i}{p} \text{tr}(S(Y^tU + U^tY)) \right) \right)
\]

which by taking absolute values is bounded by

\[
\sum_{U \in \mathbb{Z}/p} \left| \sum_{Y \in \mathbb{Z}/p} \exp \left( \frac{2\pi i}{p} \text{tr}(S(Y^tU + U^tY)) \right) \right|
\]

Now, since \( S \) is symmetric, \( \text{tr}(S(A + A^t)) = 2 \text{tr}(SA) \), hence the exponent can be written as \( 4\pi i \text{tr}(SU^tU)/p \). Letting \( V = SU^t = [v_{ij}] \) and \( Y = [y_{ij}] \), the trace of \( SU^tY \) is \( \sum_{1 \leq i \leq k, 1 \leq j \leq n} v_{ij} y_{ji} \). However, the choices for \( Y \) range over the set of all \( n \) by \( k \) matrices. Thus, for a particular \((i, j)\) pair, the value of \( v_{ij} \) remains fixed while the value of \( y_{ji} \) ranges from 0 to \( p - 1 \), independently of the values for any other \((i, j)\) pair. Therefore the summation over all \( Y \) may be rewritten as the product over all \((i, j)\) pairs of \( \sum_{0 \leq \alpha \leq p-1} \exp((4\pi iv_{ij}/p)\alpha) \). Thus the whole expression becomes

\[
\sum_{U \in \mathbb{Z}/p} \left| \prod_{1 \leq i \leq k} \sum_{0 \leq \alpha \leq p-1} \exp \left( \frac{4\pi i}{p} v_{ij} \alpha \right) \right|
\]

Finally, if \( v_{ij} \) is not 0 modp, then since \( p \neq 2 \), neither is \( 2v_{ij} \). Then the associated exponential term is the full sum of \( p \)th roots of unity, hence is 0, making the entire product equal to 0. Alternatively, if every \( v_{ij} \) is 0, then the associated term is the sum of \( p \) 1’s, hence is \( p \). Then the entire product is \( p^{nk} \), and the expression is now

\[
p^{nk} \cdot \left| \{ U \in (\mathbb{Z}/p)^{nk} \text{ such that } SU^t \equiv 0 \} \right|
\]

To finish the estimate, consider the possible matrices \( V = U^t \) such that \( SV \equiv 0 \). Let \( V_j \) be the \( j \)th column of \( V \); then \( SV \equiv 0 \) if and only if \( SV_j \equiv 0 \) for \( 1 \leq j \leq n \). Taking the rank of \( S \) to be \( r \), there are at most \( p^{k-r} \) choices for \( V_j \). Since \( V \) can
be chosen by picking any \( n \) elements of this set of \( p^{k-r} \) choices, it follows that 
\[
|\{V \in (\mathbf{Z}/p)^{kn} \text{ such that } SV \equiv 0\}| \leq p^{nk-nr}.
\]
Thus \( |G(S)|^2 \leq p^{2nk-nr} \). QED

The main estimate will be a sum over the symmetric \( k \) by \( k \) matrices with entries in \((\mathbf{Z}/p)\); given the importance of the rank of such a matrix in the last lemma, an upper bound on the number of matrices with rank \( r \) will be computed. First is a lemma which will give a standard form for these matrices.

**Lemma 6.2** Let \( S \) be a symmetric matrix with rank \( r \), whose first \( r \) rows are linearly independent. Define \( S_r \) to be the \( r \) by \( r \) upper-left submatrix of \( S \). Then \( \det(S_r) \neq 0 \).

**Proof:** Proceed by induction. If \( r = 1 \), then given that the first row is nondegenerate, it must be shown that \( S_{11} \neq 0 \). Suppose it is, hoping for a contradiction. Since the rank of \( S \) is 1, every row must be a multiple of the first. Then, in particular, \( S_{m1} \) is a multiple of \( S_{11} \) for \( 2 \leq m \leq \dim(S) \). Therefore, the first column of \( S \) is the zero vector; however, by symmetry, this implies that the first row is the zero vector as well, a contradiction.

Now consider the general case. Let \( S_r \) be the upper-left \( r \) by \( r \) submatrix of \( S \), and let \( s = \text{rank}(S_r) \). Clearly, \( s \leq r \) and if \( s = r \) the proof is done. Otherwise, consider the subvectors \( V_i = [S_{i1}, S_{i2}, \ldots S_{ir}] \). Since the rank of \( S_r \) is \( s \), the vectors \( \{V_1, V_2, \ldots V_r\} \) are all linear combinations of some \( s \) element subset of the collection. Similarly, since \( S \) has rank \( r \) and the first \( r \) rows are linearly independent, it follows that the vectors \( V_j \) for \( j > r \) are linear combinations of \( \{V_i, 1 \leq i \leq r\} \), and hence by extension are linear combinations of an \( s \) element subset.

However, the vectors \( V_i \) for \( 1 \leq i \leq \dim(S) \) together compose the first \( r \) columns of \( S \). Then it has been shown that this set of columns has at most \( s \) linearly independent elements. Now, by symmetry, it follows that the first \( r \) rows contain at most \( s \) independent vectors, which gives a contradiction. Then \( s = r = \text{rank}(S_r) \), so it follows immediately that \( \det(S_r) \neq 0 \). QED
Lemma 6.3 The number of symmetric, $k$ by $k$ matrices with entries in $(\mathbb{Z}/p)$ and rank $r$ is bounded by $Cp^{r(r+1)/2+r(k-r)}$, where $C$ is a constant which depends only on $k$.

Proof: Let $S$ be a symmetric, $k$ by $k$ matrix with entries in $(\mathbb{Z}/p)$ and rank $r$. Note that by swapping the $i$ and $j$ rows of $S$, followed by swapping the $i$ and $j$ columns, the symmetry of $S$ is preserved while allowing any two rows to be interchanged. Therefore, choose $r$ rows of $S$ which are linearly independent, and move them to be the first rows of the matrix. This operation reduces the number of matrices under consideration by a factor which only depends on $k$.

Let $S_r$ be the $r$ by $r$ upper-left submatrix of $S$; by Lemma 6.2, $\det(S_r) \neq 0$. Suppose the entries of $S_r$ are chosen randomly. With $p$ choices for each element and the symmetry of $S_r$, this gives a total of at most $p^{r(r+1)/2}$ matrices. Similarly assume that the entries in the upper-right $r$ by $k-r$ submatrix are also chosen randomly, giving an additional factor of $p^{(k-r)}$. By symmetry, this leaves only the entries of the lower-right $k-r$ by $k-r$ submatrix to be computed.

Fix $i, j$ with $k-r \leq i, j \leq k$, $R_i = [S_{i1}, S_{i2}, \ldots S_{ir}]$ and $C_j = [S_{1j}, S_{2j}, \ldots S_{rj}]$. Then the matrix $M$ formed by combining the upper left submatrix $S_r$ with the partial row $R_i$ and the partial column $C_j$ and filling in the final entry with $S_{ij}$ is an $r+1$ by $r+1$ submatrix of $S$, which has rank $r$. Therefore, $\det(M) = 0$. Expanding the determinant in terms of the last column yields the equation $S_{ij} \det(S_r) + C = 0$, where $C$ is a constant independent of the value of $S_{ij}$. Since $\det(S_r) \neq 0$, this means that $S_{ij}$ is uniquely determined for all such $i, j$.

Therefore, the number of rank 1 matrices is bounded by the product of the number of ways to choose the $r$ independent rows, the number of possible choices for $S_r$, and the possible entries in the upper right submatrix. QED
The final lemma of this section constructs a useful characteristic function which identifies the zero matrix.

**Lemma 6.4** Let $B$ be a symmetric $k$ by $k$ matrix with entries in $(\mathbb{Z}/p)$, and define $\chi(B) = p^{-\frac{k(k+1)}{2}} \sum_{S \in (\mathbb{Z}/p)^{k^2, \text{sym}}} \exp\left(\frac{2\pi i}{p} tr(SB)\right)$. Then $\chi(B)$ equals 1 if $B = 0$, and 0 otherwise.

**Proof:** Since $B$ and $S$ are both symmetric by assumption, computing $tr(SB)$ yields $\sum_{1 \leq i,j \leq k} B_{ij} S_{ij}$. Then, as in Lemma 6.1, the sum over all choices for $S$ can be rearranged as a product over all of the $i,j$ entries of $B$, yielding $\prod_{1 \leq i,j \leq k} \sum_{1 \leq \alpha \leq p} \exp\left(\frac{2\pi i}{p} B_{ij} \alpha\right)$.

Suppose for some $i,j$ pair that $B_{ij} \neq 0$. Then for the corresponding term in the product, the summation will be of the complete set of $p$th roots of unity, hence 0. Then $\chi(B)$ would be 0. Otherwise, $B_{ij} = 0$ for all $i, j$, and the original sum degenerates to $\sum_{S \in (\mathbb{Z}/p)^{k^2, \text{sym}}} 1$. There are $p^{\frac{k(k+1)}{2}}$ choices for $S$, hence $\chi(B) = 1$.

**QED**

### 6.3 Solutions for Large Primes

The problem under investigation is to show that there exist $n$ by $k$ matrices $X$ such that $X^t X = T$, where $X$ and $T$ have entries in $(\mathbb{Z}/p)$ and $T$ is symmetric and positive definite. Let $N(T)$ be the number of distinct choices for $X$ which satisfy the equation; then the goal is to find an asymptotic estimate for this function.
Thus, noting that $X^tX - T$ is always symmetric if $T$ is, and applying Lemmas 6.4 and 6.1, $N(T) = \# \{ X \in (\mathbb{Z}/p)^{kn} \text{ such that } X^tX = T \}$ becomes

$$
p^{-(k+1)/2} \sum_{X \in (\mathbb{Z}/p)^{kn}} \sum_{S \in (\mathbb{Z}/p)^{k^2, \text{sym}}} \exp \left( \frac{2\pi i}{p} \text{tr}(S(X^tX - T)) \right)
= p^{-(k+1)/2} \sum_{S \in (\mathbb{Z}/p)^{k^2, \text{sym}}} \exp \left( -\frac{2\pi i}{p} \text{tr}(ST) \right) \sum_{X \in (\mathbb{Z}/p)^{kn}} \exp \left( \frac{2\pi i}{p} \text{tr}(SX^tX) \right)
= p^{-(k+1)/2} \sum_{S \in (\mathbb{Z}/p)^{k^2, \text{sym}}} \exp \left( -\frac{2\pi i}{p} \text{tr}(ST) \right) G(S)
$$

Define $N_r(T)$ as $N(T)$, but with the choices for $S$ further reduced to those matrices of rank $r$. Hence, $N(T) = \sum_{0 \leq r \leq k} N_r(T)$. Applying Lemma 6.3 gives an immediate bound of

$$N_r(T) \leq p^{-(k+1)/2} C_k p^{r(k+1) + r(k-n) + k(n-k-1)/2}
\leq C_k p^{-(k+1)/2} C_k p^{k(n-k-1)/2}
$$

If $n \geq 2k + 1$, then

$$N_r(T) \leq C_k p^{-k(n-k-1)/2}$$

Furthermore, if $r \geq 2$, then $N_r(T) \leq C_k p^{nk-k(k+1)/2-2}$, which will form the error term in the estimate for $N(T)$. Correspondingly, since the zero matrix is the only matrix of rank 0 and $G(0) = p^{nk}$, it follows that $N_0(T) = p^{nk-k(k+1)/2}$, which will be the major term. However, getting an acceptable estimate for $N(T)$ when $n = 2k + 1$ will require a sharper bound at $r = 1$ than this analysis provides.

First is a classification of the matrices $Y$ with rank 1. Suppose the first row of $Y$ is non-zero. Then by Lemma 6.2, $Y_{11} \neq 0$. Let $y = Y_{11}$ and let $y_i = Y_{1i}/y$ for $1 \leq i \leq k$. Since every row is a multiple of the first, symmetry requires that row $i$ be $y_i$ times the first. Therefore, $Y_{ij} = y_i y_j$ for $1 \leq i, j \leq k$.

If the first row is the zero vector, then the first column is zero as well, and the problem can be reduced to considering the matrix $[Y_{ij}]$, $2 \leq i, j \leq k$. This reduction
may be repeated as many times as necessary, however it will terminate by the \(k\)th step since otherwise \(Y\) would be the zero matrix which does not have rank 1. As a consequence, there are at most \(p - 1\) choices for \(y\), \(p^{k-1}\) choices for the \(y_i\) with \(2 \leq i \leq k\) (noting that \(y_1 = 1\)), and at most \(k\) reductions that can be made. Thus, there are at most \(k(p - 1)p^{k-1}\) matrices of rank 1.

With this notation in place, \(N_1(T)\) may be calculated, starting with explicitly computing the Gaussian Sum.

**Lemma 6.5** Let \(G(Y) = \sum_{X \in \mathbb{Z}/p} \exp \left( \frac{2\pi i}{p} \text{tr}(YX^tX) \right)\), with \(Y\) of rank 1. Then \(G(Y) = p^{n(k-1)}G_p^n \left( \frac{y}{p} \right)\), where \(G_p\) is the standard Gaussian Sum of a single variable, and \(\left( \frac{y}{p} \right)\) is the quadratic residue symbol for \(y\) with respect to \(p\).

**Proof:** Let \(X_i\) denote the \(i\)th row of \(X\). Then \(\text{tr}(YX^tX) = \sum_{1 \leq i,j \leq k} Y_{ij}X_i \cdot X_j = y \sum_{1 \leq i,j \leq k} y_i y_j X_i \cdot X_j\). Splitting the sum up into a product between the \(i\) and \(j\) terms simplifies this expression as

\[
y \left| \sum_{1 \leq i \leq k} y_i X_i \right|^2.
\]

Now, \(\sum_{1 \leq i \leq k} y_i X_i\) is simply a vector, hence its norm can be written as the sum of the squares of the coordinates: \(\sum_{1 \leq i \leq k} \left( \sum_{1 \leq j \leq k} y_j X_{ji} \right)^2\).

Substituting this expression in for the trace yields

\[
G(Y) = \sum_{X \in \mathbb{Z}/p} \exp \left( \frac{2\pi i}{p} y \sum_{1 \leq i \leq k} \left( \sum_{1 \leq j \leq k} y_j X_{ji} \right)^2 \right)
\]

Since the summation is over all possible \(n\) by \(k\) matrices, it may be further decomposed as a product of \(n\) identical summations giving

\[
G(Y) = \left( \sum_{X \in \mathbb{Z}/p} \exp \left( \frac{2\pi i}{p} y \left( \sum_{1 \leq i \leq k} y_i x_i \right) \right) \right)^n = \Gamma_k(y)^n
\]

To calculate \(\Gamma_k(y)\), observe that \(\sum_{1 \leq i \leq k} y_i x_i = x_1 + \sum_{2 \leq i \leq k} y_i x_i = a\) has a total of \(p^{k-1}\) solutions for any particular value of \(a\). This follows because \(x_i\) may be chosen freely for \(2 \leq i \leq k\), but then the value of \(x_1\) is set. Therefore \(\Gamma_k(y) = \)
\[ p^{k-1} \sum_{1 \leq a \leq p} \exp \left( \frac{2\pi i}{p} ya^2 \right) = p^{k-1} \left( \frac{a}{p} \right) G_p. \]

Finally, \[ G(Y) = \Gamma_k(y)^n = p^{n(k-1)} G_p \left( \frac{y}{p} \right), \]

where the power on the quadratic residue has been reduced since \( n = 2k + 1 \) is odd.

**QED**

Substituting in the value for \( G(Y) \) into \( N_1(T) \) yields

\[ p^{-\frac{k(k+1)}{2}} p^{n(k-1)} G_p \sum_{Y \in (\mathbb{Z}/p)^2, \text{rank } 1} \exp \left( -\frac{2\pi i}{p} \text{tr}(YT) \right) \left( \frac{y}{p} \right) \]

Now use the classification of rank 1 matrices to break up the sum over the variables \( y \in (\mathbb{Z}/p)^*, y_1 = 1 \) and \( y_i \in (\mathbb{Z}/p) \) for \( 2 \leq i \leq k \)

\[ p^{-\frac{k(k+1)}{2}} p^{n(k-1)} G_p \sum_{[y_2, \ldots, y_k] \in (\mathbb{Z}/p)^{k-1}} \sum_{y \in (\mathbb{Z}/p)^*} \exp \left( -\frac{2\pi i}{p} \sum_{1 \leq i,j \leq k} (yy_i y_T y_{ij}) \right) \left( \frac{y}{p} \right) \]

\[ = p^{-\frac{k(k+1)}{2}} p^{n(k-1)} G_p \sum_{[y_2, \ldots, y_k] \in (\mathbb{Z}/p)^{k-1}} \sum_{y \in (\mathbb{Z}/p)^*} \exp \left( -\frac{2\pi i}{p} yC_{ij} \right) \left( \frac{y}{p} \right) \]

where \( C_{ij} \) is a constant based upon \( T \) and the values \( y_i \).

Then the inner sum over \( y \) is a standard Gaussian Sum; hence has a magnitude of \( \sqrt{p} \) if \( C_{ij} \) is nonzero, and is 0 if \( C_{ij} = 0 \). Therefore, by taking \( G_p \) and the inner sum to both have size \( \sqrt{p} \) an upper bound for \( N_1(T) \) is

\[ p^{-\frac{k(k+1)}{2}} p^{n(k-1)} p_{\pi}^n \sum_{[y_2, \ldots, y_k] \in (\mathbb{Z}/p)^{k-1}} p^{\frac{n}{2}} \leq p^{nk - \frac{k(k+1)}{2} - \frac{n}{2}} = p^{nk - \frac{k(k+1)}{2} - 1} \]

Since \( N(T) \geq N_0(T) - \left| \sum_{1 \leq r \leq k} N_r(T) \right| \), it follows that \( N(T) \geq p^{nk - \frac{k(k+1)}{2}} (1 - C_k p^{-1}) \). In particular, for all \( p \) larger than a constant which is based only on \( k \), \( N(T) \) is positive. However, the main use of \( N(T) \) will be to estimate the number of solutions over \((\mathbb{Z}/p)^r\). However, this first requires reducing the summation slightly to obtain liftable matrices.

**Lemma 6.6** Let \( N'(T) \) be the number of matrices \( X \in (\mathbb{Z}/p)^{nk} \) of rank \( k \) such that \( X'X = T \). Then \( N'(T) \geq p^{nk - \frac{k(k+1)}{2}} (1 - C_k p^{-1}) \).
Proof: The lemma follows from showing that there are comparatively few matrices $Y$ of rank less than $k$ such that $Y'Y = T$. In particular, assume that the row $Y_k$ is a linear combination of the first $k - 1$ rows. Define $Y'$ to be $Y$ with the row $Y_k$ removed, and let $T'$ be $T$ with the last row and column removed. Then $Y'^*Y' = T'$.

But now $N(T') \leq \sum_{0 \leq r \leq k-1} |N_r(T')|$, so $N(T') \leq C_k p^{n(k-1)-\frac{(k-1)k}{2}}$, thereby bounding the number of possible choices for $Y'$. Since $Y$ depends on the choices for $Y'$ and the constants $\lambda_i$ in the linear dependency, there are at most $C_k p^{n(k-1)-\frac{(k-1)k}{2}+k-1} = C_k p^{nk-\frac{k(k+1)}{2}-n+2k-1}$ possibilities. For values of $n$ at least $2k + 1$, this implies that $N(T) - N'(T)$ is smaller than $N(t)$ by at least an order of $p^2$. QED

Using a Hensel’s Lemma style lifting, an estimate on the number of matrices which are solutions over $(\mathbb{Z}/p^r)$ follows directly.

**Theorem 6.7** Define $N(T, p, r)$ to be the number of matrices $X \in (\mathbb{Z}/p^r)^{nk}$ such that $X'X = T \mod p^r$. Then $N(T, p, r) \geq p^{rk-\frac{k(k+1)}{2}}(1 - C_k p^{-1})$ for all $p$ greater than a constant depending on $k$.

Proof: For $r = 1$ the result follows from computing $N'(T)$ for the corresponding prime $p$. Thus, it only remains to show that nonsingular matrices mod $p^r$ may be lifted to many nonsingular matrices mod $p^{r+1}$.

Let $X$ be a matrix in $(\mathbb{Z}/p^r)^{nk}$ with $X'X = T \mod p^r$ and rank($X \mod p$) = $k$. The aim is to find many choices for $U \in (\mathbb{Z}/p)^{nk}$ such that $Y = X + p^r U \in (\mathbb{Z}/p^{r+1})^{nk}$ is a solution to $Y'Y = T \mod p^{r+1}$. This equation reduces to $X'X + p^r X'U + p^r U'X + p^{2r} U^2 = X'X + p^r (X'U + U'X) = T \mod p^{r+1}$. Since $X'X \mod p^r$, it follows that $p^r (X'U + U'X) = p^r A \mod p^{r+1}$ and thus $X'U + U'X = A \mod p$, for $A = T - X'X$.

Set $V = X'U$ as a matrix in $(\mathbb{Z}/p)^{k^2}$, so that the equation further reduces to $V + V' \equiv A \mod p$. Since $T$ is symmetric, so is $A$. Equating corresponding elements
in the sum yields the equations $2V_{ii} = A_{ii}$ for $1 \leq i \leq k$ and $V_{ij} + V_{ji} = A_{ij}$ for $1 \leq i < j \leq k$. Since $2$ is invertible, the first equation implies that the values for $V_{ii}$ are already determined. However, the second equation only gives a restriction on the sum of the symmetric off-diagonal entries; therefore the upper right triangular entries may be chosen freely. This gives a total of $p^{(k-1)k/2}$ choices for $V$.

Now the question to answer is how many matrices $U$ satisfy the equation $X'U = V$ for any fixed choice of $V$. Since $U$ and $V$ are considered as matrices over $(\mathbb{Z}/p)$, let $X'$ be the reduction of $X'$ mod $p$. It is sufficient to determine how many matrices are in the kernel of $X'$. This in turn amounts to considering the kernel of $X'$ interpreted as a mapping of vectors from $(\mathbb{Z}/p)^n$ to $(\mathbb{Z}/p)^k$ because $X'$ mapping a matrix to the zero matrix is equivalent to mapping all of its column vectors to the zero vector. Since rank($X'$) = $k$, it must be that dim(ker($X'$)) = $n - k$ and thus there are on the order of $p^{n-k}$ vectors in the kernel. Hence, there are $p^{nk-k^2}$ matrices in the kernel of $X'$ as a matrix map.

Finally, this implies that there are at least $p^{nk-k^2+\frac{(k-1)k}{2}} = p^{nk-k(k+1)/2}$ choices for $U$. In turn, $N(T, p, r + 1) \geq p^{nk-k(k+1)/2}N(T, p, r)$, which proves the theorem. QED

6.4 Solutions for Small Primes

Due to the constant $C_k$ which appears in the formula for $N(T)$, the estimate is ineffective for smaller primes. This section will show that for any odd prime there is a solution to $X'X = T$ mod $p$ where $X$ has full rank. That is, there is no local obstruction to solving the problem over the integers for $n \geq 2k + 1$, except possibly for the case $p = 2$.

**Theorem 6.8** Let $p$ be a prime other than 2 and let $n = 2k + 1$. Then for any symmetric, positive definite $k$ by $k$ matrix $T$, there is a solution to $X'X = T$ over $(\mathbb{Z}/p)$ for $X \in (\mathbb{Z}/p)^{nk}$ with rank($X$) = $k$. 

**Proof:** Suppose $p \equiv 1 \mod 4$; then $a$ can be written as the sum of two squares, not both 0, in $(\mathbb{Z}/p)$ for any choice of $a$. Construct $X$ as follows.

Denote by $X_j$ the $j$th column of $X$. Then $X_1 \cdot X_1 \equiv Y_{11} \mod p$; choose $X_{11}$ and $X_{21}$, not both zero, such that $X_{11}^2 + X_{21}^2 \equiv Y_{11} \mod p$, and let $X_{j1} = 0$ for $3 \leq j \leq n$. In particular, $X_1$ is not the zero vector.

Suppose $X_1, X_2, \ldots, X_j$ have been selected, where $[X_{2m-1,i}, X_{2m,i}] \neq [0, 0]$ for $i \leq j$ and $1 \leq m \leq i$ and the remaining entries in the columns are all zero. To construct $X_{j+1}$, start with the equation $X_{j+1} \cdot X_1 = T_{1,j+1}$ and choose $X_{1,j+1}$ and $X_{2,j+1}$ not both zero such that it is satisfied. To do this, suppose without loss of generality that $X_{1,1} \neq 0$. Then $X_{1,j+1} = (T_{1,j+1} - X_{2,1}X_{2,j+1})X_{1,1}^{-1}$, a linear equation with $p$ solutions. Hence there is a solution where not both $X_{1,j+1}$ and $X_{2,j+1}$ are zero.

Now consider the equation $X_{j+1} \cdot X_2 = T_{2,j+1}$; with the first two entries of $X_{j+1}$ already selected, this reduces to $X_{3,j+1}X_{32} + X_{4,j+1}X_{42} = T_{2,j+1} - C$, where $C$ is based on the first two values from each vector. Choose $X_{3,j+1}$ and $X_{4,j+1}$ as before to satisfy this equation, and proceed in this manner until the first $2j$ elements of $X_{j+1}$ have been chosen. Then, finally consider $X_{j+1} \cdot X_{j+1} = T_{j+1,j+1}$ which reducesto $X_{j+1,2j+1} + X_{j+1,2j+2} = T_{j+1,j+1} - C'$. Select these last two entries such that they are nonzero, and fill in the remaining components of the vector with zeroes. Then $X_{j+1}$ is neccessarily independent from the prior $j$ vectors.

However, if $p \equiv 3 \mod 4$, then 0 can not be written as the sum of two nonzero squares mod $p$. This in turn shall require the additional $2k + 1$st dimension in order to obtain a solution. In particular, every number mod $p$ can be written as the sum of three squares which are not all zero, so begin by writing $T_{11}$ in this form, and take $X_{11}, X_{21}$ and $X_{31}$ to be these three values and fill the rest of column $X_1$ with zeroes.

A similar extending algorithm shall be used to obtain the $j + 1$st column from the prior $j$. In particular, $X_{1,i}$ may be chosen freely, $[X_{2m,i}, X_{2m+1,i}] \neq [0, 0]$ for $m \leq i$,
and $X_{m,i} = 0$ for $m > 2i + 1$. Suppose $X_1, X_2, \ldots, X_j$ have been created in this manner. To construct $X_{j+1}$, select $X_{1,j+1}$ freely and assume the first $2i + 1$ entries have been chosen, where $2i + 3 < 2j$. To select $X_{2i+2,j+1}$ and $X_{2i+3,j+1}$, consider the equation $X_j \cdot X_{j+1} = T_{j,j+1}$ which reduces to $X_{2i+2,j}X_{2i+2,j+1} + X_{2i+3,j}X_{2i+3,j+1} = T_{j,j+1} - C$. Since at most one of the values $X_{2i+2,j}$, $X_{2i+3,j}$ is zero, then as before, a solution to this equation may be found where at most one of $X_{2i+2,j+1}$ and $X_{2i+3,j+1}$ is zero.

Now it just remains to construct the four entries $X_{2j+1,j+1}, \ldots, X_{2j+3,j+1}$; the difficulty here is that $T_{j+1,j+1} - \sum_{1 \leq i \leq 2j+1} X_{i,j+1}^2 = 0$ would make it impossible to choose $X_{2j+2,j+1}$ and $X_{2j+3,j+1}$ nonzero, thereby making it difficult to guarantee that $X_{j+1}$ is linearly independent from the prior columns. It will be sufficient to show that there are at least two sets of choices for the pair $X_{2j,j+1}$ and $X_{2j+1,j+1}$ where the corresponding values of $X_{2j,j+1}^2 + X_{2j+1,j+1}^2$ are not congruent. Then simply choose a pair where $T_{j+1,j+1} - \sum_{1 \leq i \leq 2j+1} = \alpha \neq 0$; then write $\alpha$ as the sum of two squares, which become the values of $X_{2j+2,j+1}$ and $X_{2j+3,j+1}$.

Reduce the equation $X_j \cdot X_{j+1} = T_{j,j+1}$ to the form $X_{2j,j}X_{2j,j+1} + X_{2j+1,j}X_{2j+1,j+1} = C'$. Assume without loss of generality that $X_{2j,j} \neq 0$; thus $X_{2j,j+1} = (C' - X_{2j+1,j}X_{2j+1,j+1})X_{2j,j}^{-1}$ has $p$ solutions and at least $p - 1$ solutions where $X_{2j+1,j+1} \neq 0$. For simplicity let $\chi = X_{2j+1,j+1}, b = C'X_{2j,j}^{-1}$ and $c = X_{2j+1,j}X_{2j,j}^{-1}$ so that $X_{2j,j+1}^2 + X_{2j+1,j+1}^2 = (b - c\chi)^2 + \chi^2 = \chi^2(1 + c^2) - 2bc\chi + b^2$. Replacing $\chi$ by $\chi + 1$ changes this expression by a value of $(2\chi + 1)(1 + c^2) - 2bc$, which needs to be nonzero. Noting that $1 + c^2 \neq 0$, this gives a single problematic value for $\chi$, which can be ignored as long as

$p > 3$ or $\chi \neq 1$.

In the case where $p = 3$, additional care must be taken when choosing the $X_{2i-2,i}$ and $X_{2i-1,i}$ entries. Make the additional assumption that $[X_{2i-2,i}, X_{2i-1,i}]$ and $[X_{2i-2,i+1}, X_{2i-1,i+1}]$ are linearly independent. This can be assured when creating
By adding the requirement that $X_{2j+1,j+1} \neq X_{2j+1,j}X_{2j,j}^{-1}X_{2j,j+1}$. Substituting this expression into the representation for $X_{2j+1,j+1}$ in the last paragraph yields $X_{2j,j+1} \neq C'X_{2j,j}^{-1} - (X_{2j+1,j}X_{2j,j}^{-1})^2X_{2j,j+1}$. Since $1 + (X_{2j+1,j}X_{2j,j}^{-1})^2 \neq 0$, this equation fails for only one value of $X_{2j,j+1}$. Naturally, this is a problem if there is only one possible choice for $X_{2j,j+1}$, which in turn implies that $X_{2j+1,j} = 0$. In this case though, having chosen $X_{2j+1,j+1} \neq 0$ guarantees the desired linear independency.

The purpose now is to alter the value of $\sum_{1 \leq i < 2j-1} X_{i,j}X_{i,j+1}$; this has the effect of changing the value of $C'$, which in turn changes the problematic value of $\chi = (2bc(1 + c^2)^{-1} - 1)2^{-1}$ to something other than 1. To accomplish this, the vector $X_{j-1}$ will have to be considered as well. To simplify notation, let $x_1 = X_{2j-2,j-1}, x_2 = X_{2j-1,j-1}, y_1 = X_{2j-2,j}, y_2 = X_{2j-1,j}, z_1 = X_{2j-2,j+1}$ and $z_2 = X_{2j-2,j+1}$. Altering the value of the sum will be accomplished by choosing new values for $z_1$ and $z_2$. The argument in the last paragraph allows the assumption that $x_1y_2 - x_2y_1 \neq 0$.

Having chosen all values of $X_{m,l}$ for $m \leq 2j - 3$ and $m \leq j + 1$ means that the equations derived from $T$ reduce to $x_1y_1 + x_2y_2 = C_1, x_1z_1 + x_2z_2 = C_2$ and $y_1z_1 + y_2z_2 = C_3$. Note that the values of $C_1$ and $C_2$ must remain fixed, while the goal is to alter $C_3$. Assume without loss of generality that $x_1 \neq 0$, to derive the relationship $z_1 = (C_2 - x_2z_2)x_1^{-1}$. Substituting this into the third equation yields $C_3 = y_1(C_2 - x_2z_2)x_1^{-1} + y_2z_2 = C_2y_1x_1^{-1} + z_2(y_2 - y_1x_2x_1^{-1}).$ This is an expression of the form $C_2 = m_1 + m_2z_2$ where $m_2 \neq 0$. Therefore different values of $z_2$ will give rise to different values for $C_3$; since there are at least 2 nonzero choices for $z_2$, the desired result follows. The base case for this argument only depends on being able to do this construction when $j = 1$, which in turn follows from direct computation.

QED

Now, lifting the solutions via Hensel’s Lemma gives a solution over $\mathbb{Z}_p$ for all odd primes $p$, while the last section proves that for $p$ sufficiently large there are actually many solutions.
Chapter 7

Equidistribution of Points

The aim here is to sketch how the estimate on the number of embeddings of triangles from Theorem 4.5 applies to the equidistribution of specialized points on a class of manifolds. It must be noted that this estimate is necessary, but is only one component of the result. The other key ingredient is a recent bound by A. Toth on the Fourier Coefficients of Siegel cusp forms of degree 2. This requires sophisticated work for modular forms on the Siegel upper-half space. As such, the discussion in this chapter will be a brief sketch of the ideas involved. On a conceptual level, this follows the argument for the equidistribution of lattice points on spheres.

7.1 Description of the Manifold

Let \( n \geq 5 \), and let \((a, b, e)\) be an admissible triple. Denote by \( M_\lambda \) the subset of \( \mathbb{R}^{2n} \) given by \( \{X, Y \in \mathbb{R}^n \text{ such that } |X|^2 = \lambda a, |Y|^2 = \lambda b, XY = \lambda e\} \). Then \( M_\lambda \) may be described as the set of embeddings of a scaled triangle into \( \mathbb{R}^n \), with centers at the origin.

Then \( M \) is a homogeneous space, acted on by the rotation group \( SO(n) \). Indeed, for any rotation \( U \in SO(n) \) and any embedding \( X, Y \), then \( UX, UY \) gives another embedding. Also, since any triangle may be rotated freely in \( \mathbb{R}^n \), the action is transitive.

Considering that any element of \( SO(n) \) which leaves a triangle fixed must also leave the plane that triangle sits in fixed, it follows that the stabilizer is isomorphic to
Therefore, \( M \) may also be considered as a realization of \( SO(n)/SO(n-2) \). Finally, \( M \) inherits the Haar measure from \( SO(n) \), yielding a unique normalized rotation invariant measure \( d\mu \) on \( M \).

Embedding the triangle \((a, b, e)\) into \( \mathbb{Z}^n \) then amounts to finding the intersection \( M \cap \mathbb{Z}^{2n} \). For any \( M_\lambda \) this gives a collection of lattice points \( L_\lambda \). Since \( M_\lambda = \sqrt{\lambda}M_1 \), it is natural to consider how these points vary as \( \lambda \) grows larger. The result under study is that as \( \lambda \to \infty \), with \( \lambda \) odd, the points \( N_\lambda/\sqrt{\lambda} \) become equidistributed over \( M \). In particular, for \( \phi \) a continuous function on \( M \)

\[
\lim_{\lambda \to \infty, \lambda \text{ odd}} \frac{1}{|N_\lambda|} \sum_{|X, Y| \in (M_\lambda \cap \mathbb{Z}^{2n})} \phi \left( \frac{X}{\sqrt{\lambda}}, \frac{Y}{\sqrt{\lambda}} \right) = \int_M \phi(x, y)d\mu(x, y) \tag{7.1}
\]

7.2 Harmonic Functions

By the Stone-Weierstrass Theorem, it is sufficient to show that Equation 7.1 holds for polynomials, and thus to show it for homogeneous polynomials. For the spheres version of the argument, this was further reduced to spherical harmonics. However, for this higher codimensional result, homogeneous pluri-harmonic polynomials must be considered. These are functions \( P(Z) : \mathbb{C}^{2n} \to \mathbb{C} \) under the condition that for every 2 by 2 matrix \( B \in \mathbb{C}^4 \), \( P_B(Z) = P(BZ) \) is harmonic. That is, \( \Delta P_B = \sum_{1 \leq i, j \leq n} \left( \frac{\partial^2 P}{\partial x_i \partial x_j} \right)^2 = 0 \). Define \( H_{k,n} \) to be the space of such polynomials which are homogeneous of degree \( k \).

Two fairly fundamental facts need to be used.

**Lemma 7.1** Let \( M \) be a manifold associated to a fixed triangle.

i) If \( P \) is a homogeneous polynomial of degree \( k \), then its restriction to \( M \) can be written as \( P|_M = \sum_{j \leq k/2} P_{k-2j}|_M \), where \( P_{k-2j} \in H_{k-2j,n} \).

ii) If \( P_k \in H_{k,n} \) and \( k \geq 1 \) then \( \int_M P_k(Z)d\mu(Z) = 0 \).

**Sketch:** For \( i \), there is an inner product to be used on the set of polynomials given by \( \langle Q, P \rangle = [Q(\delta_{x_1}^{\delta_{x_1}}, \ldots, \delta_{x_i}^{\delta_{x_i}}), \ldots)P](0) \); that is, let \( Q \) become an operator
applied to $P$, where the variables of $Q$ are now partial derivatives. This gives a new polynomial, which is then evaluated at the origin.

Also to be used is the decomposition of $P_k^*$, the space of all homogeneous polynomials of degree $k$, into $(P_k^* - 2|X|^2 + P_k^* - 2XY + P_k^* - 2|Y|^2) \perp H_k$. Since the polynomials $|X|^2, XY$ and $|Y|^2$ are constant on $M$, this result follows by induction.

For $ii)$, start with the Mean Value Property for harmonic functions:

$$P(0) = \frac{1}{(2\pi)^n} \int_{\mathbb{R}^{2n}} \exp \left( -\frac{1}{2} \text{tr}(Z^tZ) \right) P(Z) dX$$

Now if $P(Z)$ is pluri-harmonic and homogeneous of degree $k \geq 1$, then the above may be applied to $P_B(Z)$ to obtain

$$0 = \int_{\mathbb{R}^{2n}} \exp \left( -\frac{1}{2} \text{tr}(Z^tYZ) \right) P(Z) dX$$

where $Y = B^tB$ is a positive matrix. Considering the right side of the equation as a function of $Y$ extends to a holomorphic function on the half-space $G = Y + iU$, with $U$ symmetric. Therefore, the equation remains valid for such matrices $G$ in place of $Y$ as well.

Then, writing $M$ as $\{ Z \in \mathbb{R}^{2n} \text{ such that } Z^tZ = A = \begin{bmatrix} a & e \\ e & b \end{bmatrix} \}$ (with the interpretation that an $n$ by 2 matrix $Z$ has columns $X$ and $Y$ which give an embedding of the triangle into $\mathbb{R}^n$), the integral to be evaluated becomes

$$\int_{Z^tZ=A} P(Z) d\mu(Z) = C_A \int_{Z^tZ=A} \exp \left( -2\pi \text{tr}(Z^tZ) \right) P(Z) d\mu(Z)$$

$$= C_A' \int_{\mathbb{R}^{2n}} \int_{\mathbb{R}^{3}} \exp \left( -2\pi \text{tr}(Z^tZ) \right) \exp \left( 2\pi i \text{tr}((Z^tZ - A)U) \right) P(Z) dU dZ$$

where the latter equality stems from the Fourier Inversion formula for $\mathbb{R}^3$ considered as the space of 2 by 2 symmetric matrices. Changing the order of integration, the inner integral becomes of the form in Equation 7.2 with $G = 4\pi(I + iU)$, hence is 0.

QED
7.3 Equidistribution

Since Equation 7.1 is clearly true for constants, it just remains to show that

$$\frac{1}{|N_\lambda|} \sum_{Z \in \mathbb{Z}^{2n}, Z^t Z = \lambda A} P_k \left( \frac{Z}{\sqrt{\lambda}} \right) \to 0, \quad \text{as } \lambda \to \infty, \text{ odd}$$

for $P_k \in H_{k,n}, k \geq 1$. Theorem 4.5 gives that $|N_\lambda| \geq C \lambda^{n-3-\epsilon}$.

Then the result follows from A. Toth’s general theorem: if $f(Z)$ is a holomorphic cusp form (possibly vector valued) of weight $h > 3$ with respect to a congruence subgroup $\Gamma \leq \text{Sp}(4, \mathbb{Z})$ on the Siegel upper-half space $H^2$, then its Fourier coefficients satisfy the estimates

$$|\hat{f}(B)| \leq C |\text{det}(B)|^{\frac{h-1}{2} + \epsilon}$$

for every $\epsilon > 0$. Basic facts about Siegel modular forms are described in Klingen and Freitag. Note that since modular forms are periodic, they have the natural Fourier expansion

$$f(Z) = \sum_{B \geq 0} \hat{f}(B) \exp(2\pi i \text{tr}(BZ))$$

where $Z = X + iY, Y > 0$ and $X$ is symmetric.

The connection is made visible by considering $N(P, B) = \sum_{Z^t Z = B} P(Z)$. Note that if $\deg(P) = k$ is odd, then $N(P, B) = 0$. This follows from the fact that if $Z^t Z = B$ then $(-Z)^t (-Z) = B$, but then $P(Z)$ and $P(-Z) = -P(Z)$ are both in the summation. Therefore, assume that $k \geq 2$ and even. Now for $P \in H_{k,n}$ let

$$\theta_P(Z) = \sum_{B > 0} \exp(\pi i \text{tr}(BZ)) N(P, B)$$

$$= \sum_{X \in \mathbb{Z}^{2n}} \exp(\pi i \text{tr}(X^t XZ)) P(X)$$

This is referred to as the theta function attached to the pluri-harmonic polynomial $P$, and its Fourier coefficients are given by $\hat{\theta_P}(B) = N(P, B)$. This theta function has remarkable transformation properties which make it a modular form; it is in fact
a cusp form of weight \( h = \frac{n}{2} + \frac{k}{2} \). Then by A. Toth and the homogeneity of \( P \),

\[
\left| \sum_{Z' Z = \lambda A} P \left( \frac{Z}{\sqrt{\lambda}} \right) \right| \leq C_{A \lambda^{\frac{n}{2} - 1 + \epsilon}}
\]

Since this sum grows more slowly than \(|N_{\lambda}|\), the equidistribution result holds.


[12] Toth, A (To be published) *Fourier Coefficients of Siegel Modular Forms of Degree 2*. 
The following program was written to determine what choices for \((a, b, e)\) and \(n\) represent a triangle embeddable in \(\mathbb{Z}^n\). Comments in the file describe the specific details, however the basic approach is to write \(a\) and \(b\) as the sum of \(n\) squares, and to take these vector solutions and determine what possible values of \(e\) can ensue. For the particular case \(n = 5\), values of \(a\) and \(b\) up to 500 were checked, and all admissable values of \(e\) were found.

/*
 * This program is in partial completion of the requirements of
 * my doctorate in the Department of Mathematics at the
 * University of Georgia.
 *
 * Jim Blair
 */

/*
 * The primary question is given the lengths and the dot product
 * of two vectors, can we embed them in \(\mathbb{Z}^n\) for some value of \(n\)?
 * 
 * Given \(n\) and some ranges for the values of \(a\) and \(b\) (the
 * squares of the lengths of the sides) and \(e\) (the dot product),
 * this program answers that question exactly via exhaustive
 * search.
 * 
 * Variation involving ranges of values for \(a\) and \(b\) and \(e\) are
 * also provided.
 */
// Standard #includes
#include <stdio.h>
#include <math.h>
#include <malloc.h>
#include <stdlib.h>

// This is the maximum size we allow an array to have. 
// This then effectively becomes the maximum value of n. 
#define ARR_SIZE 15

// The output file 
#define OUTPUT "output.txt"

// Each LINK contains a representation of a number as the
// sum of n squares. By using a linked list, we can record
// all the ways of writing a number as the sum of n squares, 
// effectively in one variable. 'curr' is purely a short term
// variable, used while the list is being generated. 
struct LINK {
    int curr;
    int list[ARR_SIZE];
    struct LINK *next;
} top;

// A couple of variables that we wish to have globally. 
int flag;
LINK *curr_link = NULL;
FILE *fp;

// Standard function prototyping 
// Utility functions
int factorial(int n);
void permutation(int x, int n, int *arr);
void generate_sum_list(int a, int n);
void recurse_sum_list(int a, int n, int max);

// The main computing function 
void compute_products(LINK first, LINK second, int n, int e,
    int file, int mode);
// User input gathering routines
void process_triangle();
void process_e_values(int file);
void process_multiple_triangles(int file);
void process_grid(int file);

// The main routine just determines what calculations the user
// wants to perform, and then passes the program off to the
// appropriate function.
int main () {
    int mode, file;
    char ch;

    // Initialize the global list
    top.curr = 0;
    top.next = NULL;

    // Basic information for the user
    printf("This program assists in determining what triangles \n\nmay be embedded\n\nin an integer lattice. For greater detail, please see Jim \nBlair’s\n\ndissertation.\n\nAs a reminder, 'a' and 'b' are the squares of the lengths of \n\ntwo of\n\nthe sides of the triangle. 'e' is the dot product of these \n\ntwo vectors\n\nand 'n' is the dimension of the lattice. All four numbers \n\nshould be\n\nintegers.\n\n\n");

    while (1) {
        printf("Select one of the following computations:\n\n1) See if a given set of values for a, b, e and n result \n\nin an embeddable\n\ntriangle.\n\n2) Give values for a, b and n, and check to see if there are \n\nany admissible\n\nvalues of e for which the triangle (a,b,e,n) is <not> \n\nembeddable.\n\n3) Give values for a and n, and a range of possible values for \n\n");
        // Further processing...
    }
}
b.
All possible triangles (a,b,e,n) are tested to see whether they are embeddable or not.
4) Give the value of n, and a range of possible values for a and b.
All possible triangles (a,b,e,n) are tested to see whether they are embeddable or not.
5) Exit the program.
Select 1-5: ");
scanf("%d", &mode);

if ((mode < 1) || (mode > 5)) {
    printf("Invalid choice.\n");
    continue;
}

if (mode == 5) {
    printf("Exiting.\n");
    return 1;
}

if (mode != 1) {
    fflush(stdin);
    printf("\nDo you wish to have output redirected to a file? [y/N]\n");
    scanf("%c", &ch);
    if (ch == 'y' || ch == 'Y') file = 1;
    else file = 0;
}

printf("\n");

if (mode == 1) process_triangle();
else if (mode == 2) process_e_values(file);
else if (mode == 3) process_multiple_triangles(file);
else if (mode == 4) process_grid(file);
}
/* The main utility functions */

// The standard recursive factorial function
int factorial (int n) {
    if (n <= 0) return 1;
    if (n == 1) return 1;
    return (n * factorial(n-1));
}

// This permutation function takes a given array 'arr' and fills
// it with a permutation in (1 3 2 4) form.
// Each integer 'x' is considered to represent a unique
// permutation (e.g. 1 -> (1), 2 -> (2 1), etc). Thus, we fill
// in arr with this permutation applied to the first n integers.
void permutation (int x, int n, int *arr) {
    int i, j;
    int tmp, tmp_arr[ARR_SIZE];

    // First, initialize the arrays
    for (i = 0; i < ARR_SIZE; i++) {
        arr[i] = 0;
        tmp_arr[i] = 0;
    }

    // Consider x mod (n-i)! [no loss of information occurs because
    // of the multiplicative nature of the moduli]. tmp = x/(n-i-1)!
    // represents the value to which the ith integer should be
    // assigned.
    for (i = 0; i < n; i++) {
        x = x % factorial(n-i);
        if (i == n) tmp = 0;
        else tmp = x / factorial(n-i-1);
        // However, if this value has already been assigned out, we
        // reduce the entry to the first unassigned value.
        for (j = 0; tmp >= 0; j++)
            if (tmp_arr[j] == 0) tmp--;
        j--;
        arr[i] = j;
        tmp_arr[j] = 1;
    }
void generate_sum_list (int a, int n) {
    int max, i;

    // The data will be stored in the list pointed to by 'top'.
    curr_link = &top;
    // It's impossible for any entry in the list to be greater
    // than sqrt(a).
    max = (int) sqrt(a);
    max = (int) sqrt(a);

    // We loop from max down to 1, assuming that i is the value of
    // r_1. Then recurse, passing along information on what number
    // we are now trying to sum to (a - i^2 since r_1 is i), as well
    // as how many more terms are allowed, and what the maximum
    // value of the next term can be.
    for (i = max; i > 0; i--) {
        curr_link->list[0] = i;
        curr_link->curr = 1;
        recurse_sum_list(a - i*i, n-1, i);
    }
}

// The recursive part of the summing routine.
// 'a' is the number we're trying to sum to currently, 'n' is
// how many terms we have left to use, and local_max tells us
// what the maximum value of any of those terms can be.
void recurse_sum_list (int a, int n, int local_max) {
    int max, i, j;

    // If we've only got 1 term left, then 'a' must be a perfect
    // square. If it isn't, then this way of writing 'a' as n
    // squares failed, and we return.
    if (n == 1) {
        // These next two functions are responsible for filling the
        // curr_link list with all the fundamental ways of writing 'a'
        // as the sum of 'n' squares. By fundamental, we mean that
        // a = r_1^2 + r_2^2 + ... + r_n^2 with r_1 >= r_2 >= ... >= r_n
        // >= 0. Any way of writing a as the sum of n squares will
        // then simply be a permutation of one of the entries on this
        // list, up to +/- values of the r_i.
max = (int) sqrt(a);
if (max > local_max) {
    curr_link->curr--;
    return;
}
// However, if a is a perfect square, then we have written our
// original value of a as the sum of n squares successfully.
// Keep the data, and start another attempt.
if (a == max*max) {
    curr_link->list[curr_link->curr] = max;
    curr_link->next = (LINK *)malloc(sizeof(LINK));
    if (!curr_link->next) {
        printf("Memory allocation error.\n");
        exit(-1);
    }
    curr_link->next->curr = curr_link->curr;
    for (j = 0; j < ARR_SIZE; j++)
        curr_link->next->list[j] = curr_link->list[j];
    curr_link->next->next = NULL;
    curr_link = curr_link->next;
    flag = 1;
}
curr_link->curr--;
return;
}

// As we did in the initialization stage of the recursion, we
// start with i as large as possible, and then reduce it down
// until we exhaust the possible set of r_i’s.
max = (int) sqrt(a);
if (max > local_max) max = local_max;

for (i = max; i >= 0; i--) {
    curr_link->list[curr_link->curr] = i;
    curr_link->curr++;
    recurse_sum_list(a - i*i, n-1, i);
}
curr_link->curr--;
return;
void compute_products (LINK first, LINK second, int n, int e, int file, int mode) {

  // arr is a temporary data array
  // results is a list of flags, which are set based on the dot
  // products which are found.
  // perm is an array which holds data for a particular
  // permutation
  int arr[ARR_SIZE], results[2000], perm[ARR_SIZE];

  // a general list of variables
  int i, j, k, l, s, tmp;

  // Data structures to loop over the lists of vectors
  LINK *first_pos, *second_pos;

  // We take a look at 'first' and 'second' to determine what 'a'
  // and 'b' we are working with.
  int a, b;

  // Clean out the arrays
  for (i = 0; i < ARR_SIZE; i++)
    arr[i] = 0;

  for (i = 0; i < 2000; i++)
    results[i] = 0;

  // Recover the values of a and b.
  a = 0; b = 0;
  for (i = 0; i < n; i++) {
    a += first.list[i] * first.list[i];
    b += second.list[i] * second.list[i];
  }

  // And begin looping
  first_pos = &first;
  second_pos = &second;
while (first_pos->next != NULL) {
    while (second_pos->next != NULL) {

        // We have to account for any ordering of the entries in the
        // vectors, hence we loop over all possible permutations. Note
        // that we only need to apply this to one vector, since
        // permuting both would be the same as permuting one as we loop
        // over all possibilities.
        for (i = 0; i < factorial(n); i++) {
            permutation(i, n, perm);

            for (j = 0; j < ARR_SIZE; j++)
                arr[j] = first_pos->list[j] * 
                          second_pos->list[perm[j]];

        // The other scenario we need to take into account is whether
        // each component of the vector is positive or negative. Again,
        // since we consider all possibilities, we only need to negate
        // values in one of the vectors.
        for (k = 0; k < (1 << n); k++) {
            tmp = 0;
            for (l = 0; l < n; l++)
                if (k & (1 << l)) tmp += arr[l];
                else tmp -= arr[l];

        // Finally, since taking B -> -B would take e -> -e, we only
        // need to consider those dot products which are >= 0. This
        // also saves us from having to consider half of the +/- sign
        // possibilities.
        if (tmp < 0) tmp = -tmp;

        // Flag the resulting e value as having been found.
        results[tmp] = 1;

        // If looking for a single triangle, output the matches
        if (mode == 1 && tmp == e) {
            printf("Match:\n   a:");
            for (s = 0; s < n; s++) {
                printf(" %d", first_pos->list[s]);
            }

            if (s == n-1)
                printf("\n   b:");
            else printf(",");
        }
    }
}
for (s = 0; s < n; s++) {
    printf(" %d", second_pos->list[perm[s]]);
    if (s == n-1)
        printf("\n\n");
    else printf(",");
}

second_pos = second_pos->next;

first_pos = first_pos->next;
second_pos = &second;

// Start outputting information, based on what mode of
// calculation we are in.
if (mode == 1) {
    if (!results[e])
        printf("Triangle NOT found.\n");
    else printf("Triangle found.\n");
    return;
}

e = (int) ((float) (a + b - (sqrt(a) - sqrt(b)) * 
    (sqrt(a) - sqrt(b))) / 2.0);
flag = 0;
for (i = 0; i <= e; i++) {
    if (!results[i]) {
        if (mode == 2) {
            if (file)
                fprintf(fp, "Did not find a solution for e = \n%3d.\n", i);
            else printf("Did not find a solution for e = \n%3d.\n", i);
        } 
        else {
            if (file)
                fprintf(fp, "X");
            else printf("X");
        }
    }
if (mode != 3) return;
flag++;
} else if (mode == 3) {
    if (file)
        fprintf(fp, ".");
    else printf(".");
}

if (!flag) {
    if (mode == 2) {
        if (file)
            fprintf(fp, "All values of e found acceptable.\n");
        else printf("All values of e found acceptable.\n");
    }
    else if (mode == 4) {
        if (file)
            fprintf(fp, ".");
        else printf(".");
    }
    } // Subroutines for gathering information from the user.
void process_triangle () {
    int a, b, e, n, i;
    LINK first, second;

    printf("Select a value for a: ");
    scanf("%d", &a);
    if (a <= 0) {
        printf("Invalid choice.\n");
        return;
    }

    printf("Select a value for b: ");
    scanf("%d", &b);
    if (b <= 0) {
        printf("Invalid choice.\n");

}
return;
}

printf("Select a value for e: ");
scanf("%d", &e);
if (e < 0) {
    printf("Invalid choice.\n");
    return;
}

printf("Select a value for n: ");
scanf("%d", &n);
if (n <= 1) {
    printf("Invalid choice.\n");
    return;
}

// Now that the basic data is entered, generate the lists
// of vectors of length sqrt(a) and sqrt(b).
generate_sum_list(a, n);
first.curr = top.curr;
for (i = 0; i < ARR_SIZE; i++)
    first.list[i] = top.list[i];
first.next = top.next;

generate_sum_list(b, n);
second.curr = top.curr;
for (i = 0; i < ARR_SIZE; i++)
    second.list[i] = top.list[i];
second.next = top.next;

// And pass off to the compute_products function
compute_products(first, second, n, e, 0, 1);
}

// This function starts running over all reasonable values for e
void process_e_values (int file) {
    int a, b, n, i;
    LINK first, second;

    // We now might pring out to a file, so open it up first.
    if (file) {

fp = fopen(OUTPUT, "w");
if (fp == NULL) {
");
    exit(-1);
}

printf("\nSelect a value for a: ");
scanf("%d", &a);
if (a <= 0) {
    printf("Invalid choice.\n");
    return;
}

printf("Select a value for b: ");
scanf("%d", &b);
if (b <= 0) {
    printf("Invalid choice.\n");
    return;
}

printf("Select a value for n: ");
scanf("%d", &n);
if (n <= 1) {
    printf("Invalid choice.\n");
    return;
}

// Load up the vectors associated to a and b
generate_sum_list(a, n);
first.curr = top.curr;
for (i = 0; i < ARR_SIZE; i++)
    first.list[i] = top.list[i];
first.next = top.next;

generate_sum_list(b, n);
second.curr = top.curr;
for (i = 0; i < ARR_SIZE; i++)
    second.list[i] = top.list[i];
second.next = top.next;

// Pass off to the compute products function
compute_products(first, second, n, 0, file, 2);

// And clear out the file pointer if necessary.
if (file) {
    fflush(fp);
    fclose(fp);
}

// Now, we let b and e range over various values
void process_multiple_triangles (int file) {
    int a, min, max, n, b;
    int i;
    LINK first, second;

    // Open up the file if necessary
    if (file) {
        fp = fopen(OUTPUT, "w");
        if (fp == NULL) {
            fprintf(stderr, "Error opening file. Exiting.\n");
            exit(-1);
        }
    }

    // And start reading in the basic data from the user
    printf("Select a value for a: ");
    scanf("%d", &a);
    if (a <= 0) {
        printf("Invalid choice.\n");
        return;
    }

    printf("Select a minimum value for b: ");
    scanf("%d", &min);
    if (min <= 0) {
        printf("Invalid choice.\n");
        return;
    }

    printf("Select a maximum value for b: ");
    scanf("%d", &max);
    if (max < min) {

printf("Invalid choice.
");
return;
}

printf("Select a value for n: ");
scanf("%d", &n);
if (n <= 1) {
    printf("Invalid choice.
");
    return;
}

// Go ahead and generate the list of vectors for a, since they
// won't change
generate_sum_list(a, n);
first.curr = top.curr;
for (i = 0; i < ARR_SIZE; i++)
    first.list[i] = top.list[i];
first.next = top.next;

// Now, loop over the values for b, and compute the products.
for (b = min; b <= max; b++) {
    generate_sum_list(b, n);
    second.curr = top.curr;
    for (i = 0; i < ARR_SIZE; i++)
        second.list[i] = top.list[i];
    second.next = top.next;

    if (file)
        fprintf(fp, "%3d: ", b);
    else printf("%3d: ", b);

    compute_products(first, second, n, 0, file, 3);

    if (file)
        fprintf(fp, "\n");
    else printf("\n");
}

if (file) {
    fflush(fp);
    fclose(fp);
}
// Now, we shall allow a and b and e to range over many values.
void process_grid (int file) {
    int min_a, max_a, min_b, max_b, n, a, b;
    int i;
    LINK first, second;

    // Open up the file if necessary
    if (file) {
        fp = fopen(OUTPUT, "w");
        if (fp == NULL) {
");
            exit(-1);
        }
    }

    // Read in the values from the user
    printf("Select a minimum value for a: ");
    scanf("%d", &min_a);
    if (min_a <= 1) {
        printf("Invalid choice.
");
        return;
    }

    printf("Select a maximum value for a: ");
    scanf("%d", &max_a);
    if (max_a < min_a) {
        printf("Invalid choice.
");
        return;
    }

    printf("Select a minimum value for b: ");
    scanf("%d", &min_b);
    if (min_b <= 0) {
        printf("Invalid choice.
");
        return;
    }

    printf("Select a maximum value for b: ");
    scanf("%d", &max_b);
    if (max_b < min_b) {
        printf("Invalid choice.
");
        return;
    }
printf("Select a value for n: ");
scanf("%d", &n);
if (n <= 1) {
  printf("Invalid choice.\n");
  return;
}

// Now start looping over the values for a and b, and pass the
// code over to compute products
for (a = min_a; a <= max_a; a++) {
  generate_sum_list(a, n);
  first.curr = top.curr;
  for (i = 0; i < ARR_SIZE; i++)
    first.list[i] = top.list[i];
  first.next = top.next;

  for (b = min_b; b <= max_b; b++) {
    generate_sum_list(b, n);
    second.curr = top.curr;
    for (i = 0; i < ARR_SIZE; i++)
      second.list[i] = top.list[i];
    second.next = top.next;

    compute_products(first, second, n, 0, file, 4);
  }
}

if (file)
  fflush(fp);
else printf("\n");

if (file) {
  fflush(fp);
  fclose(fp);
}