POLYGONAL NUMBERS

by

Overtone Chipatala

B.Soc., University of Malawi, Malawi, 2000

M.B.A., Lincoln University, Jefferson City, 2004

A REPORT

submitted in partial fulfillment of the
requirements for the degree

MASTER OF SCIENCE

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2016

Approved by:

Major Professor
Todd Cochrane

Copyright

Abstract

Polygonal numbers are nonnegative integers constructed and represented by geometrical arrangements of equally spaced points that form regular polygons. These numbers were originally studied by Pythagoras, with their long history dating from 570 B.C, and are often referred to by the Greek mathematicians. During the ancient period, polygonal numbers were described by units which were expressed by dots or pebbles arranged to form geometrical polygons. In his "Introductio Arithmetica", Nicomachus of Gerasa (c. 100 A.D), thoroughly discussed polygonal numbers. Other Greek authors who did remarkable work on the numbers include Theon of Smyrna (c. 130 A.D), and Diophantus of Alexandria (c. 250 A.D).

Polygonal numbers are widely applied and related to various mathematical concepts. The primary purpose of this report is to define and discuss polygonal numbers in application and relation to some of these concepts. For instance, among other topics, the report describes what triangle numbers are and provides many interesting properties and identities that they satisfy. Sums of squares, including Lagrange's Four Squares Theorem, and Legendre's Three Squares Theorem are included in the paper as well. Finally, the report introduces and proves its main theorems, Gauss' Eureka Theorem and Cauchy's Polygonal Number Theorem.

Table of Contents

List of Figures

Acknowledgments

I would like to express my heartfelt gratitude to my major professor, Dr. Todd Cochrane for his unwavering guidance and support during the completion of this report.

Furthermore, I would also like to extend my sincere appreciation to Dr. Christopher Pinner and Dr. Craig Spencer, who were on my committee, for all of their contributions.

Many thanks also go to my family and friends for their inspiration in the preparation of the report.

Chapter 1

Introduction

Polygonal numbers are nonnegative integers represented by geometrical arrangements of equally spaced points that form regular polygons as shown below in Figure 1.1. A common starting point is identified from which the sides expand by increasing the number of points in successive polygons. The size of the polygons increase as the sum of equidistant points used to represent it grows in a common pattern. The most common and basic types of polygonal numbers are triangular and square numbers.

The triangular numbers count the number of dots in such a way that when two dots are added to a starting point, an equilateral triangle is formed. By adding three dots to the previous three points, we can obtain a larger equilateral triangle with six points. A triangle with ten dots can be created by adding four points to the six points triangle, and so on. Continuing with this augmenting arrays of dots whereby dots are well arranged forming an expanded equilateral triangle with respective sum of dots in each such triangle, results in a sequence of numbers $1, 3, 6, 10, 15, 21, 28, ...$ known as triangular numbers. Similarly, as the numbers three, five, seven, nine, etc. are added to a starting dot, forming a square array as the figure grows outwardly, the sequence of square numbers $1, 4, 9, 16, 25, 36, 49, ...$ is created. For pentagonal numbers $1, 5, 12, 22, 35, 51, 70, 92, ...$ we need to add four, seven, ten, thirteen dots and so on to a point arranged in a pentagonal form. More polygonal numbers can be constructed by continuing this procedure. Thus for any positive integer $k \geq 3$ we can form

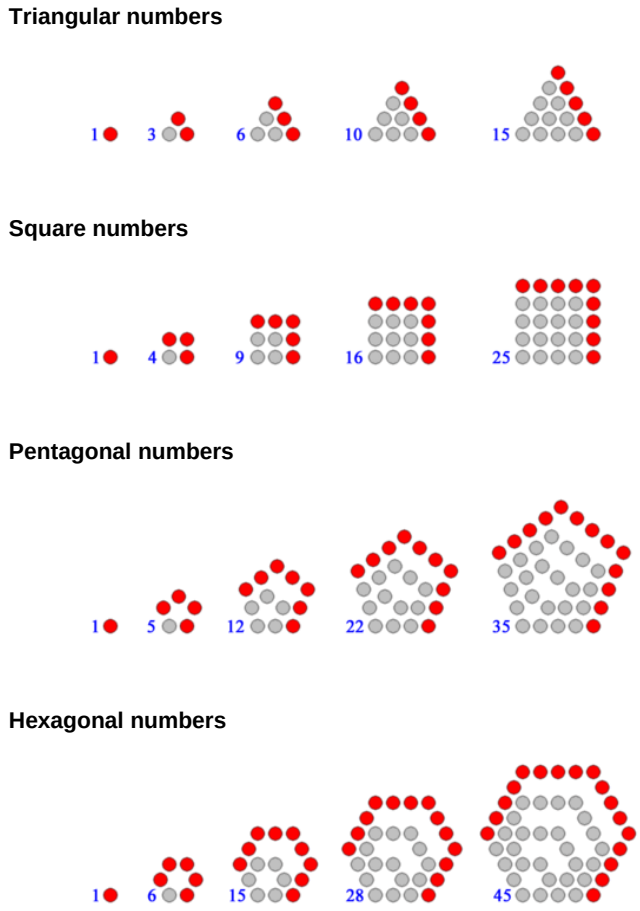


Figure 1.1: *Geometric Representations of Polygonal Numbers*[13]

a sequence of k-gonal numbers that correspond to every regular polygon with k sides.

1.1 Formula for the k-gonal numbers

Polygonal Numbers can be defined geometrically by counting the number of dots in a regular k-gon as shown in Figure 1.1. For $k \geq 3$, a k-gonal number is the total number of dots inside one of the regular k-gons in the figure. Let $P_n = P_n^{(k)}$ denote the n-th k-gonal number. For convenience we set $P_0 = 0$, $P_1 = 1$. When the context makes it clear that we are dealing with k-gons we drop the superscript $^{(k)}$ from our notation. For small k the polygonal numbers are also called triangular numbers ($k = 3$), square numbers ($k = 4$), pentagonal numbers ($k = 5$), hexagonal numbers ($k = 6$), and so on.

The k-gons in Figure 1.1 and consequently the values of the P_n are constructed recursively as follows. We start by designating a vertex point, called the base point. For the diagram below, this is the point in the lower left corner. Suppose that the first n regular k-gons have already been constructed, so that each edge of the outermost k-gonal now has length n-dots. To construct the $(n+1)$-st k-gon, first we extend the two edges attached to the base point by one dot, and then add edges parallel to the previous edges, so that each (outer) edge now has $n+1$ dots. The total number of dots we are adding to the figure is $1 + (k-2)n$. Thus we have the relation,

$$P_{n+1} = P_n + (k-2)n + 1. \tag{1.1}$$

We note that the recurrence holds as well for $n = 0$, since $1 = P_1 = P_0 + 0 + 1$. The recurrence in (1.1) is satisfied by a quadratic polynomial $P_n = An^2 + Bn + C$ for some constants A, B and C. Since $P_0 = 0$, we must have $C = 0$. Next $P_1 = 1$ implies that $1 = A + B$, while $P_2 = k$ implies that $k = 4A + 2B$. Solving the linear system

$$A + B = 1$$

$$4A + 2B = k,$$

gives $A = \frac{2k-4}{4}$, $B = \frac{4-k}{2}$, and thus for $n \geq 0$,

$$P_n = \frac{(k-2)n^2 - (k-4)n}{2}. \tag{1.2}$$

1.2 Brief history of polygonal numbers

The theory of polygonal numbers dates back at least as far as Pythagoras who was credited with the original work on the theory. He initiated the concept that polygonal numbers are derived from a gnomon (a form which, when added geometrically to a figure, gives another expanded figure similar to the original). By using the notion of polygonal numbers, Pythagoras came up with his well known theorem known as the Pythagorean Theorem. He discovered that the sum of the areas of two squares placed along the adjacent sides of a right triangle equals the area of a square placed along the hypotenuse[6] p.80,? . Thus, he established his famous and widely used formula that $a^2+b^2 = c^2$, where a and b are the lengths of the adjacent sides and c is the length of the hypotenuse of a right triangle. Unfortunately, there is no concrete source for Pythagoras' claims since all the writings that have survived the test of time about the Pythagoreans come from centuries later. Many other mathematical formulations have deep roots in polygonal numbers and several famous theorems are based on these numbers. In particular, such natural numbers as perfect numbers, Mersenne numbers, Fermat numbers, Fibonacci and Lucas numbers, etc. are related to polygonal numbers. Furthermore, a modern application of polygonal numbers is seen in Pascal's triangle and the binomial theorem. By using such numbers, coefficients that arise in binomial expansions (binomial coefficients) are displayed in the pattern of a triangle (commonly known as Pascal triangle), in which one can clearly spot the triangular numbers.

One of the Greek mathematicians, Hypsicles of Alexandria gave the first general definition of the concept of a k-gonal number in the 170 BC[6] p. 126. Hypsicles was later quoted and credited by Diophantus as being the author of polygonal numbers. During his studies on polygonal numbers, Diophantus discovered the formula we derived above for the n-th k-gonal number, $P_n = \frac{(k-2)n^2-(k-4)n}{2}$. Other classical mathematicians who had interest in polygonal

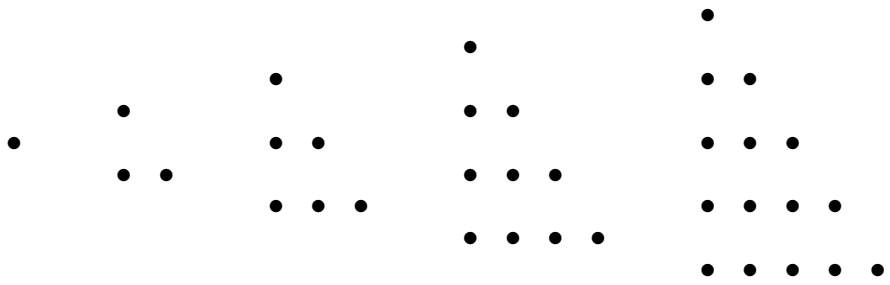
numbers include Nicomachus of Gerasa (60 - 120), Theon of Smyrna (70 - 135), and Leonardo Fibonacci (1170 - 1250), just to mention a few.

The modern study of polygonal numbers date back as far as Pierre de Fermat (1601 - 1665), who in 1636 conjectured the famous Polygonal Number Theorem which mathematicians have greatly used. In his theorem, Fermat proposed that for any $k \geq 3$, every whole number can be expressed as the sum of at most k, k-gonal numbers. Even though he claimed to have proved the theorem, no one has ever found his proof. Lagrange (1770) proved that every nonnegative integer is the sum of four squares. In 1796, Legendre and Gauss determined the numbers that can be represented as the sum of three squares, from which one readily deduces that every positive integer is a sum of at most three triangular numbers. Augustin-Louis Cauchy, published (1813) the first proof of the Polygonal Number Theorem in its entirety. Thus the theorem is sometimes called Fermat's Polygonal Number Theorem, and sometimes called Cauchy's Polygonal Number Theorem. We shall provide the proof of the Polygonal Number Theorem in this report.

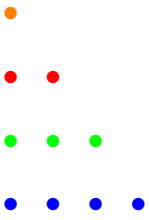
Chapter 2

Triangle Numbers

The triangle numbers (or triangular numbers) 1, 3, 6, 10, 15, 21, 36, and so on, and can be represented by dots in a triangle as shown below.



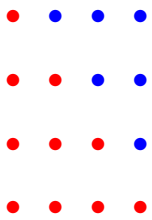
The differences between consecutive triangle numbers (including 0) are just the natural numbers 1, 2, 3, 4,... , and consequently the n-th triangle number can be viewed as the sum of the first n natural numbers, as illustrated below.



$$T_n = 1 + 2 + 3 + 4 + \cdots + n$$

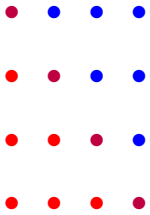
2.1 Relations between triangle numbers and squares

The figure below illustrates that the sum of two consecutive triangle numbers is a square:



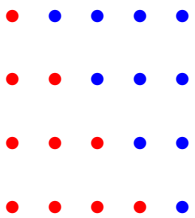
$$T_{n-1} + T_n = n^2.$$

The next figure breaks up a square into two overlapping triangles, allowing us to derive the formula for T_n:



$$n^2 = T_n + T_n - n \quad \Rightarrow \quad T_n = \frac{1}{2}(n^2 + n) = \frac{n(n+1)}{2}.$$

A more direct way to derive the formula for T_n is to break up a rectangle into two triangles as illustrated below:



$$2T_n = n(n+1) \quad \Rightarrow \quad T_n = \frac{n(n+1)}{2}.$$

Putting the above observations together yields a proof of the formula for the sum of the first n natural numbers,

$$1 + 2 + 3 + \cdots + n = T_n = \frac{n(n+1)}{2}.$$

2.2 A test for when a number is a triangle number

Theorem 2.2.1. *A positive integer n is triangular if and only if $8n + 1$ is a perfect square.*

Proof. Suppose that n is triangular. Then $n = \frac{k(k+1)}{2}$ for some $k \in \mathbb{N}$.

$$\Rightarrow 2n = k^2 + k$$
$$\Rightarrow 8n + 1 = 4k^2 + 4k + 1 = (2k + 1)^2,$$

and so $8n + 1$ is a perfect square.

Conversely, assume $8n+1$ is a perfect square. That is, $8n+1 = m^2$, for some odd positive integer m. We need to show that there is $k \in \mathbb{N}$ with $n = T_k$, that is, $n = \frac{k(k+1)}{2}$. Now, m is odd, so $m = 2k + 1$ for some $k \in \mathbb{N}$. Then

$$\begin{aligned} 8n &= (2k + 1)^2 - 1 \\ &= 4k^2 + 4k + 1 - 1 \\ &= 4k(k + 1), \end{aligned}$$

which implies that $n = \frac{k(k+1)}{2}$. Therefore, n is a triangle number. □

2.3 Triangle numbers that are squares

In this section we characterize all triangle numbers that are perfect squares. We must solve the equation

$$\frac{x(x + 1)}{2} = y^2. \tag{2.1}$$

This is equivalent to

$$(2x + 1)^2 = 8y^2 + 1,$$

Setting $X = 2x + 1$, $Y = 2y$, our task then is to solve the Pell equation

$$X^2 - 2Y^2 = 1, \tag{2.2}$$

in positive integers with X odd and Y even. Viewing the equation as a congruence (mod 4), it is plain that any solution of (2.2) must have X odd and Y even, and thus our task is simply to find all positive integer solutions of (2.2).

Let $\delta : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$ be the norm map $\delta(X + Y\sqrt{2}) = X^2 - 2Y^2$. Solving the Pell equation amounts to finding the units in $\mathbb{Z}[\sqrt{2}]$ of norm 1. From the theory of Pell equations, we know that there exists a fundamental unit $u_0 \in \mathbb{Z}[\sqrt{2}]$ such that every solution of the equation $\delta(u) = \pm 1$ is of the form $\pm u_0^n$ with $n \in \mathbb{Z}$. Moreover, if we take u_0 to be the minimal unit strictly greater than one, then every solution with positive X, Y is of the form u_0^n with $n \in \mathbb{N}$. Plainly $u_0 = 1 + \sqrt{2}$ and thus $u_0^2 = 3 + 2\sqrt{2}$ generates all solutions $u = X + Y\sqrt{2}$ of the equation $\delta(u) = 1$, with positive X and Y. For $n \in \mathbb{N}$, set $X_n + Y_n\sqrt{2} = u_0^{2n}$, so that every positive solution of (2.2) is of the form (X_n, Y_n). Put $\overline{u}_0 = 1 - \sqrt{2}$. Then

$$\begin{aligned} X_n &= \frac{1}{2}\left(u_0^{2n} + \overline{u}^{2n}\right) = \frac{1}{2}\left((3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n\right) \\ Y_n &= \frac{1}{2\sqrt{2}}\left(u_0^{2n} - \overline{u}^{2n}\right) = \frac{1}{2\sqrt{2}}\left((3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n\right), \end{aligned}$$

and consequently the positive solutions to (2.1) are given by

$$\begin{aligned} x_n &= \frac{(3 + 2\sqrt{2})^n - 2}{4} + \frac{(3 - 2\sqrt{2})^n}{4} \\ y_n &= \frac{(3 + 2\sqrt{2})^n}{4\sqrt{2}} - \frac{(3 - 2\sqrt{2})^n}{4\sqrt{2}}. \end{aligned}$$

A nice way to think about the solutions is to let $NI(x)$ denote the nearest integer to x. Then

$$x_n = NI\left(\frac{(3+2\sqrt{2})^n - 2}{4}\right)$$
$$y_n = NI\left(\frac{(3+2\sqrt{2})^n}{4\sqrt{2}}\right).$$

2.3.1 Special sequence of triangle numbers that are squares

We claim that if T is a given triangle number that is a perfect square then so is $4T(8T+1)$. Thus if we start with $T = 1$, we obtain by recursion the sequence $1, 36, 41616, \ldots$, of triangle numbers that are perfect squares. It is plain that $4T(8T+1)$ is a triangle number, indeed $4T(8T+1) = T_n$ with $n = 8T$. To see that it is a perfect square we simply appeal to Theorem 2.2.1. Since T is triangular, $8T+1$ is a perfect square. Thus $4T(8T+1)$ is a perfect square since T itself is a square.

2.4 Triangle numbers and Pascal's Triangle

The triangular numbers 1,3,6,10,15,... appear as the third southwesterly diagonal in Pascal's triangle as can be seen in the diagram below. Recall that an entry in Pascal's triangle is obtained by adding the two numbers above it.

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}
\quad ,
$$

$$
\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array}
$$

$$
\begin{array}{ccccccccccccccc}
 & & & & & & & 1 & & & & & & & \\
 & & & & & & 1 & & 1 & & & & & & \\
 & & & & & 1 & & 2 & & 1 & & & & & \\
 & & & & 1 & & 3 & & 3 & & 1 & & & & \\
 & & & 1 & & 4 & & 6 & & 4 & & 1 & & & \\
 & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & \\
 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & \\
1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1
\end{array}
$$

$$
\begin{array}{ccccccccccccccccc}
 & & & & & & & & 1 & & & & & & & & \\
 & & & & & & & 1 & & 1 & & & & & & & \\
 & & & & & & 1 & & 2 & & 1 & & & & & & \\
 & & & & & 1 & & 3 & & 3 & & 1 & & & & & \\
 & & & & 1 & & 4 & & 6 & & 4 & & 1 & & & & \\
 & & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & & \\
 & & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & & \\
 & 1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 & \\
1 & & 8 & & 28 & & 56 & & 70 & & 56 & & 28 & & 8 & & 1
\end{array}
$$

The numbers in the fourth southwesterly diagonal, 1,4,10,20,35,56,... are called Tetrahedral numbers. The n-th Tetrahedral Number H_n is the number of points in a 3-dimensional pyramid obtained by starting with a triangle base containing T_n points and then stacking triangles with $T_{n-1}, T_{n-2} \ldots, T_1$ points on top of it. Thus

$$H_n := T_1 + T_2 + \cdots + T_n.$$

This identity also illustrates the *Hockey Stick Identity* for Pascal's triangle, which states that the sum of the numbers down a diagonal of Pascal's Triangle (starting with 1) equals the number in the next row shifted one place to the right (for a southwesterly diagonal).

Recall that the values in Pascal's triangle can also be viewed as binomial coefficients. If we call [1,1] the first row of the triangle, [1,2,1] the second row and so on, the entries in the n-th row are the coefficients in the binomial expansion of $(x+y)^n$. To be precise, the k-th entry in the n-th row is $\binom{n}{k-1}$, the number of ways of choosing $k-1$ objects from a collection of n objects. The Triangle numbers are binomial coefficients with $k=3$, and we have $T_n = \binom{n+1}{2} = \frac{(n+1)n}{2}$. The tetrahedral numbers are the binomial coefficients with $k=4$, and we have $H_n = \binom{n+2}{3} = \frac{(n+2)(n+1)n}{6}$.

Theorem 2.4.1. $T_1 + \cdots + T_n = \binom{n+2}{3}$.

Proof. This identity is immediate from the definition of H_n and the fact that H_n can be represented as a binomial coefficient. We present here a direct proof using induction. For $n = 1$ the identity is trivial $T_1 = 1 = \binom{3}{3}$. Suppose the statement is true for n and consider $n + 1$. We want to show that $H_{n+1} = \binom{n+3}{3} = \frac{(n+1)(n+2)(n+3)}{6}$. Now

$$\begin{aligned} H_{n+1} &= T_1 + T_2 + \cdots + T_n + T_{n+1} \\ &= H_n + T_{n+1} = \frac{n(n+1)(n+2)}{6} + \frac{(n+1)(n+2)}{2} \\ &= \frac{n(n+1)(n+2)}{6} + \frac{3(n+1)(n+2)}{6} = \frac{n(n+1)(n+2) + 3(n+1)(n+2)}{6} \\ &= \frac{(n+1)(n+2)(n+3)}{6}. \end{aligned}$$

Thus, $H_{n+1} = \binom{n+3}{3}$. □

2.5 What numbers are sums of two triangle numbers

Theorem 2.5.1. *A positive integer n is a sum of two triangle numbers if and only if $4n+1$ is a sum of two squares.*

Proof. Suppose n is a sum of two triangle numbers. Then for some $x, y \in \mathbb{N}$, $n = \frac{x(x+1)}{2} + \frac{y(y+1)}{2} = \frac{x^2+x+y^2+y}{2}$

$$\begin{aligned} &\Rightarrow 2n = x^2 + x + y^2 + y \\ &\Rightarrow 4n + 1 = \frac{4x^2 + 4x + 4y^2 + 4y + 2}{2} = 2x^2 + 2x + 2y^2 + 2y + 1 \end{aligned}$$

Next,

$$\begin{aligned}((x+y)+1)^2+(y-x)^2 &= x^2+y^2+2xy+2x+2y+1+y^2+x^2-2xy \\ &= 2x^2+2y^2+2x+2y+1 = 4n+1.\end{aligned}$$

Thus, $4n+1=(x+y+1)^2+(y-x)^2$, a sum of two squares.

Conversely, assume $4n+1=u^2+v^2$. Our goal is to show that n is the sum of two triangle numbers. We may assume $u>v\geq 0$. Following the first part of the proof, we let $u=x+y+1$, and $v=-x+y$. Solving the linear system for x, y

$$\begin{aligned}x+y &= -1+u \\ -x+y &= v,\end{aligned}$$

gives $y=\frac{u+v-1}{2}\geq 0$, and $x=\frac{u-v-1}{2}\geq 0$. Since $4n+1=u^2+v^2$, $u^2+v^2\equiv 1 \pmod 4$ then either u is even and v is odd or u is odd and v even. This implies that

$$\begin{aligned}u+v-1 &\equiv 0 \pmod 2 \\ u-v-1 &\equiv 0 \pmod 2.\end{aligned}$$

Thus, x and y are nonnegative integers and so T_x, T_y are well defined triangle numbers. Note

that

$$\begin{aligned} T_x + T_y &= \frac{x(x+1)}{2} + \frac{y(y+1)}{2} \\ &= \frac{1}{2}\left(\frac{(u-v)-1}{2}\right)\left(\frac{(u-v)+1}{2}\right) + \frac{1}{2}\left(\frac{(u+v)-1}{2}\right)\left(\frac{(u+v)+1}{2}\right) \\ &= \frac{1}{8}\left((u-v)^2 - 1 + (u+v)^2 - 1\right) \\ &= \frac{1}{8}\left(2u^2 + 2v^2 - 2\right) = \frac{u^2+v^2-1}{4} = n \end{aligned}$$

□

2.6 Further facts about triangle numbers

Theorem 2.6.1. *The sum of the reciprocals of the triangle numbers is 2.*

Proof. The n-th triangle number T_n is given by $T_n = \frac{n(n+1)}{2}$, and so we need to show that $\sum_{n=1}^{\infty} \frac{1}{T_n} = \sum_{n=1}^{\infty} \frac{2}{n(n+1)} = 2$. Note that $\frac{2}{n(n+1)} = \frac{2}{n} - \frac{2}{n+1}$, and so for any positive integer N,

$$\begin{aligned} \sum_{n=1}^{N} \frac{1}{T_n} &= \sum_{n=1}^{N} \left(\frac{2}{n} - \frac{2}{n+1}\right) \\ &= \left(\frac{2}{1} - \frac{2}{2}\right) + \left(\frac{2}{2} - \frac{2}{3}\right) + \left(\frac{2}{3} - \frac{2}{4}\right) + ... + \left(\frac{2}{N} - \frac{2}{N+1}\right) \\ &= \frac{2}{1} - \frac{2}{2} + \frac{2}{2} - \frac{2}{3} + \frac{2}{3} - \frac{2}{4} + ... + \frac{2}{N} - \frac{2}{N+1} = 2 - \frac{2}{N+1}. \end{aligned}$$

This implies that

$$\sum_{n=1}^{\infty} \frac{1}{T_n} = \lim_{N\to\infty} 2 - \frac{2}{N+1} = 2.$$

□

Theorem 2.6.2. *For any positive integers m, n, we have*

i) $T_{m+n} = T_m + T_n + mn$.

ii) $T_{mn} = T_m T_n + T_{m-1} T_{n-1}$.

iii) $T_{2n} = 3T_n + T_{n-1}$.

iv) $T_{2n+1} = 3T_n + T_{n+1}$.

Proof. i) We have $T_m = \frac{m(m+1)}{2}$, and $T_n = \frac{n(n+1)}{2}$ for any positive integers m, n. Also $T_{m+n} = \frac{(m+n)(m+n+1)}{2}$. Therefore, we need to show that $T_m + T_n + mn = \frac{(m+n)(m+n+1)}{2}$.

$$\begin{aligned} T_m + T_n + mn &= \frac{m(m+1)}{2} + \frac{n(n+1)}{2} + mn \\ &= \frac{m^2 + m + n^2 + n + 2mn}{2} \\ &= \frac{(m^2 + 2mn + n^2) + (m+n)}{2} \\ &= \frac{(m+n)(m+n) + (m+n)}{2} \\ &= \frac{(m+n)(m+n+1)}{2} \end{aligned}$$

as desired.

ii) Similarly, for $T_{mn} = T_m T_n + T_{m-1} T_{n-1}$, we need to show that $T_m T_n + T_{m-1} T_{n-1} = \frac{mn(mn+1)}{2}$.

$$\begin{aligned} T_m T_n + T_{m-1} T_{n-1} &= \frac{m(m+1)}{2}\frac{n(n+1)}{2} + \frac{m(m-1)}{2}\frac{n(n-1)}{2} \\ &= \frac{m(m+1)n(n+1) + m(m-1)n(n-1)}{4} \\ &= \frac{(m^2+m)(n^2+n) + (m^2-m)(n^2-n)}{4} \\ &= \frac{m^2n^2 + m^2n + n^2m + mn + m^2n^2 - m^2n - n^2m + mn}{4} \\ &= \frac{2m^2n^2 + 2mn}{4} \\ &= \frac{mn(mn+1)}{2} = T_{mn}. \end{aligned}$$

iii) Also, for $T_{2n} = 3T_n + T_{n-1}$, we have $T_{2n} = \frac{2n(2n+1)}{2} = n(2n+1)$, while

$$\begin{aligned} 3T_n + T_{n-1} &= \frac{3n(n+1)}{2} + \frac{n(n-1)}{2} = \frac{3n(n+1) + n(n-1)}{2} \\ &= \frac{3n^2 + 3n + n^2 - n}{2} = \frac{4n^2 + 2n}{2} \\ &= \frac{2n(2n+1)}{2} = n(2n+1) = T_{2n}. \end{aligned}$$

iv) For $T_{2n+1} = 3T_n + T_{n+1}$, we have $T_{2n+1} = \frac{(2n+1)(2n+2)}{2} = (2n+1)(n+1)$, while

$$\begin{aligned} 3T_n + T_{n+1} &= \frac{3n(n+1)}{2} + \frac{(n+1)(n+2)}{2} = \frac{3n(n+1) + (n+1)(n+2)}{2} \\ &= \frac{(n+1)(3n+n+2)}{2} = \frac{2(n+1)(2n+1)}{2} = (n+1)(2n+1) = T_{2n+1}. \end{aligned}$$

□

Chapter 3

Sums of Two Squares

3.1 When is a number a sum of two squares

Our goal in this section is to characterize all integers that can be expressed as a sum of two squares of integers. Suppose that n is a sum of squares, $n = a^2 + b^2$. Since any square is congruent to 0 or 1 $\pmod 4$, $n \equiv a^2 + b^2 \equiv 0, 1$ or 2 $\pmod 4$. Thus we have a necessary condition for n to be a sum of two squares. Unfortunately, this is not a sufficient condition. For example $6 \equiv 2 \pmod 4$, $12 \equiv 0 \pmod 4$ and $21 \equiv 1 \pmod 4$ but 6,12 and 21 are not sums of two squares. The problem is that 6, 12 and 21 have the prime factor 3, which cannot be expressed as a sum of squares. If we restrict our attention to primes then the necessary condition is sufficient.

Theorem 3.1.1. *Let p be an odd prime. Then p is a sum of two squares if and only if $p \equiv 1 \pmod 4$.*

Proof. We have already seen that $p \equiv 1 \pmod 4$ is a necessary condition, so we need only prove the converse. Suppose that $p \equiv 1 \pmod 4$. Then $(\frac{-1}{p}) = 1$ (see Appendix A), so there exists a $u \in \mathbb{Z}$ with $u^2 \equiv -1 \pmod p$. Consider the set of integers of the form $x + uy$ with $x, y \in [0, \sqrt{p}] \cap \mathbb{Z}$. Since there are $([\sqrt{p}] + 1)^2 > p$ choices for (x, y), there must exist, by the

pigeonhole principle, distinct $(x_1, y_1) \neq (x_2, y_2)$ with

$$x_1 + uy_1 \equiv x_2 + uy_2 \pmod{p}, \quad \text{that is,} \quad (x_1 - x_2) \equiv u(y_2 - y_1) \pmod{p}.$$

Set $a = x_1 - x_2$, $b = y_1 - y_2$. Then $|a| < \sqrt{p}$, $|b| < \sqrt{p}$ and $a \equiv ub \pmod{p}$. Therefore $a^2 + b^2 \equiv (1 + u^2)b^2 \equiv 0 \pmod{p}$ and $a^2 + b^2 < 2p$. Furthermore, since $(x_1, y_1) \neq (x_2, y_2)$, $a^2 + b^2 > 0$. Thus $a^2 + b^2 = p$. □

To generalize this theorem to an arbitrary positive integer, let us recall that by unique factorization, any positive integer n can be uniquely expressed in the manner $n = n_1 n_2^2$ with n_1 square-free. Indeed, if $n = \prod_{i=1}^{k} p_i^{e_i}$, then we rearrange the primes so that the first l primes occur to an odd multiplicity while the remaining occur to an even multiplicity. Then, with $e_i = 2f_i + 1$, $1 \leq i \leq l$, $e_i = 2f_i$, $l + 1 \leq i \leq k$,

$$n = \prod_{i=1}^{l} p_i^{2f_i+1} \prod_{i=l+1}^{k} p_i^{2f_i} = \prod_{i=1}^{l} p_i \prod_{i=i}^{k} p_i^{2f_i} = n_1 n_2^2,$$

where $n_1 = \prod_{i=1}^{l} p_i$, $n_2 = \prod_{i=l+1}^{k} p_i^{f_i}$.

Theorem 3.1.2. *Let n be a positive integer with $n = n_1 n_2^2$, where n_1 is square-free. Then n is a sum of two squares if and only if n_1 has no prime divisor $p \equiv 3 \pmod{4}$.*

Proof. Necessity: Let p be a prime divisor of n with $p \equiv 3 \pmod{4}$. We shall prove by induction on e that if $p^{2e+1} \| n$, then n is not a sum of two squares. Suppose $e = 0$ and that $p \| n$. If $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$, then $a^2 + b^2 \equiv 0 \pmod{p}$, and so $p|a$ and $p|b$, for otherwise we would have $(ab^{-1})^2 \equiv -1 \pmod{p}$, contradicting $\left(\frac{-1}{p}\right) = -1$. But this implies that $p^2|(a^2 + b^2)$, that is, $p^2|n$ a contradiction. Suppose the assertion is true for $e - 1$ and consider the case e. Say $p^{2e+1} \| n$. By the same argument, if $n = a^2 + b^2$ for some integers a, b then $p|a$ and $p|b$, and so $\frac{n}{p^2} = (a/p)^2 + (b/p)^2$, but this is impossible by the induction assumption. We conclude that any prime divisor p of n with $p \equiv 3 \pmod{4}$ cannot be a factor of n_1.

Sufficiency: Say $n_1 = \prod_{i=1}^{l} p_i$ where $p_i = 2$ or $p_i \equiv 1 \pmod 4$, $1 \leq i \leq l$. Then for $1 \leq i \leq l$, p_i is a sum of two squares by the previous theorem, and so $p_i = \delta(w_i)$ for some Gaussian integer w_i where $\delta(a+bi) = a^2 + b^2$. Putting $w = \prod_{i=1}^{k} w_i$ we see that $\delta(w) = n_1$ and $\delta(n_2 w) = n_2^2 \delta(w) = n$. Therefore n is a sum of two squares. □

3.2 Primitive representations as sums of two squares

Definition 3.2.1. A positive integer n is said to have a primitive representation as a sum of two squares if $n = a^2 + b^2$ for some integers a, b with $(a, b) = 1$.

Theorem 3.2.1. *A positive integer n has a primitive representation as a sum of two squares if and only if $n = n_1$ or $2n_1$ where n_1 has only prime divisors of the form $p \equiv 1 \pmod 4$.*

Proof. Suppose $n = n_1 = \prod_{i=1}^{k} p_1^{e_i}$ where the p_i are distinct primes with $p_i \equiv 1 \pmod 4$. We have $p_i = \pi_i \overline{\pi_i}$ for some prime $\pi_i = a_i + b_i i \in \mathbb{Z}[i]$, with $a_i^2 + b_i^2 = p_i$. Set $u = a + bi := \prod_{i=1}^{k} \pi_i^{e_i}$. Then u is not divisible by any rational prime and $u\overline{u} = n$, that is, $a^2 + b^2 = n$, a primitive representation of n as a sum of two squares. Likewise if $n = 2n_1$ with n_1 as above, we set $u = (1+i)\prod_{i=1}^{k} \pi_i^{e_i}$ to get a primitive representation $n = u\overline{u}$.

Conversely, suppose $n = a^2 + b^2$ with $(a, b) = 1$. Let q be prime with $q \equiv 3 \pmod 4$. If $q|n$ then $a^2 + b^2 \equiv 0 \pmod q$. Since $(a, b) = 1$, this implies that $(\frac{-1}{q}) = 1$, a contradiction. Likewise, if $4|n$ then $a^2 + b^2 \equiv 0 \pmod 4$ implies $a \equiv b \equiv 0 \pmod 2$, contradiction $(a, b) = 1$. □

Chapter 4

Sums of Three Squares

In 1797 Legendre[9] established the following simple criterion for when a positive integer is a sum of three squares.

Theorem 4.0.2. *A positive integer is a sum of three squares if and only if it is not of the form* $4^k(8m+7)$ *for some nonnegative integers* k, m.

Proof. Easy direction: Suppose that there exists a number of the form $4^k(8m+7)$ that is a sum of three squares, and let $n = 4^k(8m+7)$ be the minimal such number. Note that every square is congruent to $0, 1$ or $4 \pmod 8$ and thus a sum of three squares is always $0, 1, 2, 3, 4, 5$ or $6 \pmod 8$. Thus $k > 0$ and $4|n$. But, in order to obtain 0 as a sum of three squares $\pmod 4$, each of the squares must be even, and therefore we have integers x, y, z satisfying $(2x)^2 + (2y)^2 + (2z)^2 = 4^k(8m+7)$. Dividing by 4 gives a smaller number of the same form as a sum of three squares, a contradiction. □

To prove the converse, we follow the proof provided in[2], which is derived from more modern results, including Dirichlet's Theorem on primes in arithmetic progressions, and the Davenport-Cassels' Lemma. Implicit in the proof are the tools used to prove the Hasse-Minkowski principle. We start by proving a weaker result, namely that any positive integer not of the form $4^k(8m+7)$ is the sum of three squares of rational numbers. It suffices to do this for any odd integer not of the form $8m+7$ and for two times any such odd integer. This is equivalent to the following lemma.

Lemma 4.0.1. *If n is an odd positive integer, with $n \not\equiv 7 \pmod 8$, then there exist integers x, y, z, w with $w \neq 0$ such that*

$$x^2 + y^2 + z^2 = nw^2. \tag{4.1}$$

The same is true for the equation $x^2 + y^2 + z^2 = 2nw^2$.

Proof. We shall deduce this theorem as a consequence of another theorem of Legendre dealing with the solvability of the equation $ax^2 + by^2 = cz^2$. This theorem, which we shall simply call Legendre's Theorem here, is stated and proven in Appendix C.

We may assume that n is an odd square-free positive integer with $n \equiv 1, 3$ or $5 \pmod 8$. Write $n = \prod_{i=1}^{k} p_i = P_1 P_2$ where the p_i are distinct odd primes, $P_1 = \prod_{i=1}^{l} p_i$ is the product of primes $p_i \equiv 1 \pmod 4$, $P_2 = \prod_{l+1}^{k} p_i$ the product of primes $p_i \equiv -1 \pmod 4$.

Case i: Suppose that $n \equiv 1$ or $5 \pmod 8$. Let q be any prime with $q \equiv 1 \pmod{8P_1}$, $q \equiv -1 \pmod{P_2}$. Such a prime exists by Dirichlet's Theorem on primes in arithmetic progressions. Consider the Legendre equation

$$qu^2 = nw^2 - z^2. \tag{4.2}$$

Suppose that u, w, z is a nonzero integer solution. Since $q \equiv 1 \pmod 4$, we know q is a sum of two squares (by Theorem 3.1.2) and thus so is qu^2; say $qu^2 = x^2 + y^2$ with $x, y \in \mathbb{Z}$. Thus, $x^2 + y^2 = qu^2 = nw^2 - z^2$, that is, nw^2 is a sum of three squares.

We are left with the task of showing that (4.2) has a nonzero solution. By Legendre's Theorem (see Appendix C), (4.2) is solvable if and only if $-q$ is a square $\pmod n$, and n is a square $\pmod q$. The former holds provided that $\left(\frac{-q}{p_i}\right) = 1$ for $1 \leq i \leq k$. If $p_i \equiv 1 \pmod 4$, then since $q \equiv 1 \pmod{p_i}$, we get $\left(\frac{-q}{p_i}\right) = \left(\frac{-1}{p_i}\right) = 1$. If $p_i \equiv -1 \pmod 4$, then since $q \equiv -1 \pmod{p_i}$, we have $\left(\frac{-q}{p_i}\right) = 1$. Next, by quadratic reciprocity and the fact that $q \equiv 1 \pmod 4$,

$$\left(\frac{n}{q}\right) = \prod_{i=1}^{k} \left(\frac{p_i}{q}\right) = \prod_{i=1}^{k} \left(\frac{q}{p_i}\right) = \prod_{i=1}^{l} \left(\frac{1}{p_i}\right) \prod_{i=l+1}^{k} \left(\frac{-1}{p_i}\right) = (-1)^{k-l}.$$

Since $n \equiv 1 \pmod 4$, there must be an even number of prime divisors $p_i \equiv -1 \pmod 4$, and so $\left(\frac{n}{q}\right) = 1$, completing the proof.

Next consider the Legendre equation

$$qu^2 = 2nw^2 - z^2. \tag{4.3}$$

Again, $-q$ is a square $\pmod n$, and $-q$ is trivially a square $\pmod 2$, and so $-q$ is a square $\pmod{2n}$. To show $2n$ is a square $\pmod q$ it suffices to show that 2 is a square $\pmod q$, since we have already shown that n is a square $\pmod q$. But $q \equiv 1 \pmod 8$, and so 2 is a quadratic residue (mod q). Thus, by Legendre's Theorem, (4.3) has a nonzero solution, and so $2nw^2$ is a sum of three squares.

Case ii: Suppose that $n \equiv 3 \pmod 8$. To represent n as a sum of three rational squares, we consider the equation

$$2qu^2 = nw^2 - z^2. \tag{4.4}$$

Let q be a prime such that $q \equiv 1 \pmod 4$, and $q \equiv -2 \pmod{p_i}$, $1 \leq i \leq k$, so that

$$\left(\frac{q}{p_i}\right) = \left(\frac{-2}{p_i}\right) = \begin{cases} 1, & \text{if } p_i \equiv 1, 3 \pmod 8; \\ -1, & \text{if } p_i \equiv 5, 7 \pmod 8. \end{cases}$$

Since $q \equiv 1 \pmod 4$, we know that $2qu^2$ is a sum of two squares. Next, $-2q$ is a square $\pmod n$ by design, that is, $(\frac{-2q}{p_i}) = 1$ for all i. Finally, let n_3, n_5, n_7 denote the number of primes p_i with $p_i \equiv 3, 5, 7 \pmod 8$ respectively. Then

$$\left(\frac{n}{q}\right) = \prod_{i=1}^{k} \left(\frac{p_i}{q}\right) = \prod_{i=1}^{k} \left(\frac{q}{p_i}\right) = \prod_{i=1}^{k} \left(\frac{-2}{p_i}\right) = (-1)^{n_5+n_7}.$$

Since $n \equiv 3 \pmod 8$ we have

$$n = \prod_{i=1}^{k} p_i \equiv 3^{n_3} 5^{n_5} 7^{n_7} \equiv (-1)^{n_5+n_7} 3^{n_3+n_5} \equiv 3 \pmod 8.$$

This implies that $n_3 + n_5$ is odd and that $n_5 + n_7$ is even, whence $\left(\frac{n}{q}\right) = 1$. Thus the Legendre equation (4.4) is solvable in nonzero integers, and we obtain nw^2 as a sum of three squares.

Finally, to obtain $2n$ as a sum of three rational squares, we consider the equation

$$qu^2 = 2nw^2 - z^2. \tag{4.5}$$

Let q be a prime with $q \equiv 5 \pmod 8$ and $(\frac{q}{p_i}) = (\frac{-1}{p_i})$, for all i. Since $q \equiv 1 \pmod 4$ we once again know that qu^2 is a sum of two squares. Next, $-q$ is a square $\pmod{2n}$ since $(\frac{-q}{p_i}) = 1$ for all i and $-q$ is trivially a square $\pmod 2$. Finally,

$$\left(\frac{2n}{q}\right) = \left(\frac{2}{q}\right)\prod_{i=1}^{k}\left(\frac{p_i}{q}\right) = -\prod_{i=1}^{k}\left(\frac{q}{p_i}\right) = -\prod_{i=1}^{k}\left(\frac{-1}{p_i}\right) = (-1)^{n_3+n_5+1}.$$

Since $n \equiv 3 \pmod 8$ we must have n_3+n_5 odd, and so $\left(\frac{2n}{q}\right) = 1$. Therefore, (4.5) is solvable and we obtain $2nw^2$ as a sum of three squares.

□

To complete the proof of Theorem 4.0.2 we prove a special case of the Davenport-Cassels' Lemma[2] Lemma 222, which gives a criterion for when an integer is represented by a quadratic form over $\mathbb{Z}$, given that it is represented over $\mathbb{Q}$.

Suppose that n is any integer that can be expressed as a sum of three squares of rational numbers, that is, there is an integer solution to the equation

$$x_1^2 + x_2^2 + x_3^2 = nw^2, \tag{4.6}$$

with $w \neq 0$. Let $\mathbf{x} = (x_1, x_2, x_3)$ be an integer solution of this equation with minimal positive w. We claim that $w = 1$ and therefore n is a sum of three squares. Indeed, suppose that $w > 1$. In particular $w \nmid x_i$ for some i, else dividing each variable by w would already yield n as a sum of three squares. Let $\|\mathbf{x}\|$ denote the usual Euclidean norm,

$\|(x_1, x_2, x_3)\|^2 = x_1^2 + x_2^2 + x_3^2$. For $i = 1, 2, 3$, let y_i be a nearest integer to $\frac{x_i}{w}$, so that $|y_i - \frac{x_i}{w}| \leq \frac{1}{2}$, $\mathbf{x} \neq w\mathbf{y}$ and

$$0 < \|w\mathbf{y} - \mathbf{x}\|^2 \leq \tfrac{3}{4}w^2. \tag{4.7}$$

Let $\mathbf{x} = (x_1, x_2, x_3)$, $\mathbf{y} = (y_1, y_2, y_3)$. Set

$$\alpha := \|\mathbf{y}\|^2 - n, \qquad \beta := 2nw - 2\mathbf{x} \cdot \mathbf{y}, \qquad \mathbf{z} := \alpha\mathbf{x} + \beta\mathbf{y},$$

and note that $\alpha, \beta \in \mathbb{Z}$, $\mathbf{z} \in \mathbb{Z}^3$ and that $\mathbf{z} \neq \mathbf{0}$. Then

$$\begin{aligned} \|\mathbf{z}\|^2 &= \alpha^2\|\mathbf{x}\|^2 + 2\alpha\beta\mathbf{x} \cdot \mathbf{y} + \beta^2\|\mathbf{y}\|^2 \\ &= \alpha^2 nw^2 + 2\alpha\beta nw + \beta^2 n = n(\alpha w + \beta)^2, \end{aligned}$$

and so $\mathbf{z}$ is a solution of (4.6) with w replaced by $(\alpha w + \beta)$. We also have

$$\|w\mathbf{y} - \mathbf{x}\|^2 = w^2\|\mathbf{y}\|^2 - 2w\mathbf{x} \cdot \mathbf{y} + \|\mathbf{x}\|^2 = w^2(\alpha + n) - w(2nw - \beta) + nw^2 = w(\alpha w + \beta),$$

and so by (4.7),

$$0 < (\alpha w + \beta) \leq \tfrac{3}{4}w,$$

but this contradicts the minimality of w.

Chapter 5

Sums of Three Triangle Numbers

In this section we first show that n is a sum of three triangular numbers if and only if $8n+3$ is a sum of three squares. Then, since any positive number of the form $8n+3$ is a sum of three squares theorem, by Theorem 4.0.2, we arrive at the following theorem, called Gauss's Eureka Theorem.

Theorem 5.0.3. *(Gauss's Eureka Theorem). Every positive integer is the sum of three triangular numbers.*

Note that in the statement of the theorem we consider zero to be a triangular number. Alternatively, one could say every positive integer is a sum of at most three triangular numbers if we didn't want zero to be considered as a triangular number.

Lemma 5.0.2. *A positive integer n is a sum of three triangular numbers if and only if $8n+3$ is a sum of three squares.*

Proof. Suppose n is a sum of three triangular numbers. Then $n = \frac{k(k+1)}{2} + \frac{m(m+1)}{2} + \frac{h(h+1)}{2}$ where h, k, m are nonnegative integers. We want to show that $8n+3$ is a sum of 3 odd squares. Now $n = \frac{(k^2+k+m^2+m+h^2+h)}{2} \Leftrightarrow 2n = k^2+k+m^2+m+h^2+h \Leftrightarrow 8n = 4k^2+4k+4m^2+4m+4h^2+4h \Leftrightarrow 8n+3 = 4k^2+4k+4m^2+4m+4h^2+4h+3 = (4k^2+4k+1)+(4m^2+4m+1)+(4h^2+4h+1) = (2k+1)^2 + (2m+1)^2 + (2h+1)^2$, a sum of three squares.

Conversely, assume $8n+3 = x^2+y^2+z^2$ for some nonnegative integers x, y, z. We need to show there exists natural numbers k, m, h with $n = \frac{k(k+1)}{2} + \frac{m(m+1)}{2} + \frac{h(h+1)}{2}$, that is n is

a sum of three triangular numbers. Since $x^2 + y^2 + z^2 \equiv 3 \pmod 8$ we must have x, y, z are all odd, so $x = 2k + 1$, $y = 2m + 1$, and $z = 2h + 1$, for some nonnegative integers h, k, m. Thus, $8n+3 = (2k+1)^2+(2m+1)^2+(2h+1)^2$. Using the equivalence in the first paragraph we obtain, $n = \frac{k(k+1)}{2} + \frac{m(m+1)}{2} + \frac{h(h+1)}{2}$, as desired. □

Chapter 6

Sums of Four Squares

In 1770 Lagrange established the Four Squares Theorem:

Theorem 6.0.4. *Every positive integer is the sum of 4 squares.*

We will provide two proofs of the theorem, the first a short proof deducing it as a consequence of the Three Squares Theorem, and the second a longer proof utilizing Minkowski's Theorem from the Geometry of Numbers.

6.1 Deducing Lagrange's Theorem from the Three Squares Theorem

Let n be a positive integer. If n is not of the form $4^k(8m+7)$ for some nonnegative integers k, m, then we know that n is a sum of three squares, and thus trivially a sum of four squares using zero as the fourth square. Suppose next that $n = 4^k(8m+7)$ for some k, m. Then $n - 4^k = 4^k(8m+7) - 4^k = 4^k(8m+6)$ which is not of the form $4^{k'}(8m'+7)$ for any integers k', m'. Thus $n - 4^k = a^2 + b^2 + c^2$ for some $a, b, c \in \mathbb{Z}$, and $n = (2^k)^2 + a^2 + b^2 + c^2$.

6.2 Proving Lagrange's 4-squares Theorem using the Geometry of Numbers

In this section we use Minkowski's Theorem to deduce Lagrange's 4-squares Theorem directly, without appeal to the Three Squares Theorem.

Lemma 6.2.1. *Let p_1, p_2, p_3, p_4 be the quadratic forms in variables x_i, y_i, $1 \leq i \leq 4$, defined by the matrix equation*

$$P := \begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{bmatrix} = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ -x_2 & x_1 & -x_4 & x_3 \\ -x_3 & x_4 & x_1 & -x_2 \\ -x_4 & -x_3 & x_2 & x_1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix}.$$

Then

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = p_1^2 + p_2^2 + p_3^2 + p_4^2.$$

In particular, the product of two integers that are sums of four squares is again a sum of four squares.

Proof. Observing that the rows of the matrix M appearing in the lemma are orthogonal we see that

$$\begin{aligned} p_1^2 + p_2^2 + p_3^2 + p_4^2 = P^t P = (MY)^t MY = Y^t M^t MY = Y^t (x_1^2 + x_2^2 + x_3^2 + x_4^2) I_4 Y \\ = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2). \end{aligned}$$

□

Lemma 6.2.2. *Let γ_n denote the surface area of a sphere of radius 1 in $\mathbb{R}^n$ and β_n denote its volume. Then, for $n \geq 2$ we have $\beta_n = \gamma_n / n$ and $\gamma_{n+2} = 2\pi\beta_n$.*

Proof. The first identity $\gamma_n = n\beta_n$ is immediate, indeed if we let $\gamma_n(r)$, $\beta_n(r)$ denote the surface area and volume of a n-dimensional sphere of radius r, then $\beta_n'(r) = \frac{n}{r}\beta_n(r)$ and

$\beta_n'(r) = \gamma_n(r)$. Evaluating at $r = 1$ yields the identity. To obtain the second identity, observe that

$$\begin{aligned}(\sqrt{\pi})^n &= \left(\int_{-\infty}^{\infty} e^{-x^2}\ dx\right)^n \\ &= \int_{\mathbb{R}^n} e^{-r^2}\ dV = \int_0^{\infty} e^{-r^2}\gamma_n r^{n-1} dr \\ &= \frac{\gamma_n}{2}\int_0^{\infty} e^{-x} x^{\frac{n}{2}-1}\ dx = \frac{\gamma_n}{2}\Gamma(n/2).\end{aligned}$$

Since $\Gamma(x+1) = x\Gamma(x)$ for $x > 0$, we have $\Gamma(\frac{n}{2}+1) = \frac{n}{2}\Gamma(\frac{n}{2})$. Thus

$$\beta_n = \frac{\gamma_n}{n} = \frac{2\pi^{n/2}}{n\Gamma(n/2)} = \frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)} = \frac{1}{2\pi}\gamma_{n+2}.$$

□

Lemma 6.2.3. *For any prime p the congruence $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ has a solution.*

Proof. Let $S = \{x^2 : x \in \mathbb{F}_p\}$, $T = -1 - S$. Then $|T| = |S| = \frac{p+1}{2}$ and so $S \cap T \neq \emptyset$. □

Proof of Lagrange's Theorem. By the first lemma it suffices to prove that any prime p is a sum of four squares. Our strategy is to find a lattice of solutions of the congruence

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{p}, \tag{6.1}$$

and then apply Minkowski's theorem to pick out a small nonzero point in this lattice. Let a, b be integers satisfying $a^2 + b^2 + 1 \equiv 0 \pmod{p}$. Then $\mathbf{u}_1 := (a, b, 1, 0)$, $\mathbf{u}_2 := (b, -a, 0, 1)$ are solutions of (6.1). Also, $\mathbf{u}_3 := (p, 0, 0, 0)$ and $u_4 := (0, p, 0, 0)$ are trivially solutions. Let $\mathcal{L}$ be the lattice of points in $\mathbb{R}^n$ with basis $\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{u}_4\}$. It is easy to show that every point in $\mathcal{L}$ satisfies the congruence (6.1), and that $\Delta(\mathcal{L}) = p^2$. Let S be the sphere of radius $\sqrt{2p}$ centered at the origin in $\mathbb{R}^4$. By the above lemma,

$$Vol(S) = (\sqrt{2p})^4\beta_4 = 2\pi^2 p^2 > 2^4 p^2 = 2^4\Delta(\mathcal{L}),$$

and thus by Minkowski's Theorem (see Appendix B), S contains a nonzero point $\mathbf{x} \in \mathcal{L}$. This point satisfies $x_1^2 + x_2^2 + x_3^2 + x_4^2 = kp$ for some positive integer k, and at the same time $x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2p$. Therefore, $x_1^2 + x_2^2 + x_3^2 + x_4^2 = p$. $\square$

Chapter 7

Polygonal Number Theorem

7.1 Introduction

Fermat (1638) conjectured that for any $k \geq 3$, every positive integer can be expressed as a sum of at most k, k-gonal numbers. This was proven in full by Cauchy (1813). We will call the result the Polygonal Number Theorem, although it is often called Cauchy's Polygonal Number Theorem or Fermat's Polygonal Number Theorem.

Theorem 7.1.1. *(Polygonal Number Theorem). For any positive integer $k \geq 3$, every positive integer can be expressed as a sum of at most k, positive k-gonal numbers.*

Since we are calling 0 a k-gonal number, we could just as well have said that every positive integer is a sum of exactly k, k-gonal numbers. The proof we give here follows the work of Nathanson[10]. We start by establishing the theorem for small N (the number being represented) in the next section, and then establish it for large N in the following two sections.

We note that for any $k \geq 3$, there exist values of N that cannot be represented by fewer than k, k-gonal numbers, namely $N = 2k - 1$ (for $k \geq 3$) and $N = 5k - 4$ (for $k \neq 4$), as we shall see below.

7.2 The tables of Pepin and Dickson

Recalling the formula for the n-th k-gonal number

$$P_n = P_n^{(k)} = \frac{(k-2)n^2 - (k-4)n}{2},$$

we obtain

$$P_1 = 1, \quad P_2 = k, \quad P_3 = 3k-3, \quad P_4 = 6k-8, \quad P_5 = 10k-15, \ldots.$$

Using these values, we can represent small integers as sums of at most k, k-gonal numbers.

Pepin[12] and Dickson[3], created extensive tables showing how to represent any integer $N \leq 120k - 240$ as a sum of k, k-gonal numbers, at most four of which are different from 0 or 1. To illustrate how this table is made we will show here how to represent every natural number $N < 10k - 15 = P_5$ as a sum of k, k-gonal numbers at most four of which are different from 0 or 1. To do this we break up the interval $[1, P_5]$ into the subintervals $[P_1, P_2) = [1, k)$, $[P_2, P_3) = [k, 3k-3)$, $[P_3, P_4) = [3k-3, 6k-8)$, $[P_4, P_5) = [6k-8, 10k-15)$, $[P_5, P_6) = [10k-15, 15k-24)$.

For numbers N in the interval $[P_1, P_2) = [1, k)$, we can simply represent N as a sum of 1's,

$$\begin{aligned} 1 &= 1 && 1 \\ 2 &= 1+1 && 2 \\ &\vdots \\ k-1 &= 1+1+\cdots+1 && k-1 \end{aligned}$$

In the column on the right we have indicated the total number of nonzero k-gonal numbers used to represent N.

For $k \leq N < 3k-3$, we have $k = P_2$,

$$
\begin{aligned}
k+1 &= k+1 && 2\\
k+2 &= k+1+1 && 3\\
k+3 &= k+1+1+1 && 4\\
&\vdots\\
2k-1 &= k+1+\cdots+1 && k\\
2k &= k+k && 2\\
2k+1 &= k+k+1 && 3\\
2k+1+1 &= k+k+1+1 && 4\\
&\vdots\\
3k-4 &= k+k+1+\cdots+1 && k-2
\end{aligned}
$$

For $3k-3 \leq N < 6k-8$ we have $3k-3 = P_3$,

$$
\begin{array}{ll}
3k-2 = (3k-3)+1 & 2 \\
3k-1 = (3k-3)+1+1 & 3 \\
3k = k+k+k & 3 \\
3k+1 = k+k+k+1 & 4 \\
\vdots & \\
4k-5 = k+k+k+1+1+\cdots+1 & k-2 \\
4k-4 = k+k+k+1+1+\cdots+1 & k-1 \\
4k-3 = (3k-3)+k & 2 \\
4k-2 = (3k-3)+k+1 & 3 \\
4k-1 = (3k-3)+k+1+1 & 4 \\
4k = k+k+k+k & 4 \\
4k+1 = k+k+k+k+1 & 5 \\
\vdots & \\
5k-5 = k+k+k+k+1+1+\cdots+1 & k-1 \\
5k-4 = k+k+k+k+1+1+\cdots+1 & k \\
5k-3 = (3k-3)+k+k & 3 \\
5k-2 = (3k-3)+k+k+1 & 4 \\
5k-1 = (3k-3)+k+k+1+1 & 5 \\
\vdots & \\
6k-9 = (3k-3)+k+k+1+1+\cdots+1 & k-3
\end{array}
$$

We note that for $k = 5$, the representation above for $6k-9$ makes no sense, and so instead

we use $6k - 9 = 21 = 5 + 5 + 5 + 5 + 1$, a sum of five pentagonal numbers.

For $6k-8 \leq N < 10k-15$ we have $6k-8 = P_4$,

$$
\begin{aligned}
6k-7 &= (6k-8)+1 && 2\\
6k-6 &= (3k-3)+(3k-3) && 2\\
6k-5 &= (3k-3)+(3k-3)+1 && 3\\
&\vdots\\
7k-9 &= (3k-3)+(3k-3)+1+1+\cdots+1 && k-1\\
7k-8 &= (6k-8)+k && 2\\
7k-7 &= (6k-8)+k+1 && 3\\
7k-6 &= (3k-3)+(3k-3)+k && 3\\
7k-5 &= (3k-3)+(3k-3)+k+1 && 4\\
&\vdots\\
8k-10 &= (3k-3)+(3k-3)+k+1+1+\cdots+1 && k-1\\
8k-9 &= (3k-3)+(3k-3)+k+1+1+\cdots+1 && k\\
8k-8 &= (6k-8)+k+k && 3\\
8k-7 &= (6k-8)+k+k+1 && 4\\
8k-6 &= (3k-3)+(3k-3)+k+k && 4\\
8k-5 &= (3k-3)+(3k-3)+k+k+1 && 5\\
&\vdots\\
9k-12 &= (3k-3)+(3k-3)+k+k+1+1+\cdots+1 && k-2\\
9k-11 &= (6k-8)+(3k-3) && 2\\
9k-9 &= (3k-3)+(3k-3)+(3k-3) && 3\\
9k-8 &= (6k-8)+k+k+k && 4\\
9k-7 &= (6k-8)+k+k+k+1 && 5\\
&\vdots
\end{aligned}
$$

$$
10k-16 = (6k-8)+k+k+k+1+1+\cdots+1 \qquad k-4
$$

In the display above we assume that $k \geq 8$ (in the representation of $10k-16$ there are $k-8$ ones). For smaller k slight modifications can be made.

In the course of the investigation above we discover values that cannot be represented by fewer than k nonzero k-gonal numbers, namely $2k-1$ and $5k-4$. Consider expressing $2k-1$ as a sum of the k-gonal numbers 1, k, $3k-3$,$6k-8$, ... Certainly there can be no value larger than k, and at most one k. This forces one to use $k-1$ ones, yielding a total of k terms. For $5k-4$ we cannot use $6k-8$ since we are assuming that $k \geq 5$. Also, we can use at most one $3k-3$. This leaves $k-1$, and so we are again forced to use $k-1$ ones, for a total of k terms. Alternatively, if we didn't use $3k-3$, we would (optimally) use four k's and $k-4$ ones for a total of k terms. The value $8k-9$ requires k terms if we insist on having at most four terms greater than 1. Alternatively, we can write $8k-9 = k+k+k+k+k+k+k+1+\cdots+1$ a sum of $k-2$ k-gonal numbers.

7.3 Cauchy's Lemma

The key lemma to proving the Polygonal Number Theorem is the following.

Lemma 7.3.1. *(Cauchy's Lemma) Let k and s be odd positive integers, such that $s^2 < 4k$ and $3k < s^2 + 2s + 4$. Then there exists a nonnegative integer solution (t, u, v, w) of the system*

$$k = t^2 + u^2 + v^2 + w^2; \tag{7.1}$$

$$s = t + u + v + w. \tag{7.2}$$

Proof. Note that $3k < s^2+2s+4 \Leftrightarrow 3k < s^2+2s+2+2 \Leftrightarrow 3k-2 < (s+1)^2 \Leftrightarrow \sqrt{3k-2} < s+1$ $\Leftrightarrow \sqrt{3k-2}-1 < s$. Also, $s^2 < 4k$ is equivalent to $s < 2\sqrt{k}$. Thus the hypotheses on k and s imply that $s \in (\sqrt{3k-2}-1, 2\sqrt{k})$. Now, $s^2 < 4k$ implies $4k - s^2 > 0$, and since k and s are odd we claim that, $4k - s^2$ has the form $8l+3$ for some nonnegative integer l. To see

this, let $k = 2a + 1$, $s = 2b + 1$ with $a, b \in \mathbb{Z}$. Then

$$\begin{aligned} 4k - s^2 &= 4(2b+1) - (2a+1)^2 = 8b + 4 - 4a^2 - 4a - 1 \\ &= 8b - 4a(a+1) + 3 = 8l + 3. \end{aligned}$$

Another way of seeing this is to note that for odd k, s, $4k - s^2 \equiv 4 - 1 \equiv 3 \pmod 8$. By the Three Squares Theorem, there exist positive odd integers $x \geq y \geq z > 0$, such that $4k - s^2 = x^2 + y^2 + z^2$.

Now, for nonnegative integers x, y, z we have

$$(x+y+z)^2 \leq (x+y+z)^2 + (x-y)^2 + (x-z)^2 + (y-z)^2 = 3(x^2+y^2+z^2).$$

Thus, since $4k - s^2 = x^2 + y^2 + z^2$, we have

$$x + y + z \leq \sqrt{3(4k - s^2)}.$$

Since $s > \sqrt{3k-2} - 1$, we have $(s+1)^2 > 3k - 2$, and so $3k < s^2 + 2s + 3$, and

$$\begin{aligned} x + y + z &\leq \sqrt{12k - 3s^2} < \sqrt{4(s^2 + 2s + 3) - 3s^2} = \sqrt{s^2 + 8s + 12} \\ &< \sqrt{s^2 + 8s + 16} = s + 4. \end{aligned}$$

In other words, we have $\frac{s-x-y-z}{4} > -1$. Hence, the least integer value obtained by $\frac{s \pm x \pm y \pm z}{4}$ is nonnegative. Since x, y, z are odd numbers, $x + y + z$ is odd as well, that is, $x + y + z \equiv \pm 1 \pmod 4$. Hence, for odd s, either $s - x - y - z \equiv 0 \pmod 4$, or $s + x + y + z \equiv 0 \pmod 4$, that is, either $\frac{s-x-y-z}{4}$ or $\frac{s+x+y+z}{4}$ is an integer.

If $\frac{s-x-y-z}{4}$ is an integer, we define integers t, u, v, w by

$$\begin{aligned} t &:= \frac{s-x-y-z}{4}, \quad u := t + \frac{y+z}{2} = \frac{s-x+y+z}{4}; \\ v &:= t + \frac{x+z}{2} = \frac{s+x-y+z}{4}, \quad w := t + \frac{x+y}{2} = \frac{s+x+y-z}{4}. \end{aligned}$$

It is easy to see that $t+u+v+w=s$ and that

$$t^2+u^2+v^2+w^2=\tfrac{1}{16}\left(4(s^2+x^2+y^2+z^2)\right)=k,$$

that is, t,u,v,w is a nonnegative solution of the system above.

If $\frac{s+x+y+z}{4}$ is an integer, we define integers t,u,v,w by

$$\begin{aligned} t&:=\frac{s+x+y+z}{4}, \quad u:=t-\frac{y+z}{2}=\frac{s+x-y-z}{4};\\ v&:=t-\frac{x+z}{2}=\frac{s-x+y-z}{4}, \quad w:=t-\frac{x+y}{2}=\frac{s-x-y+z}{4}, \end{aligned}$$

and again see that t,u,v,w is a nonnegative solution of the system above. □

7.4 Proof of the Polygonal Number Theorem

We noted above that the tables of Pepin and Dickson establish that every positive $N<120k-240$ can be expressed as a sum of at most k k-gonal numbers at most four of which are different from 0 or 1. The proof of the Polygonal Number Theorem will be completed if we can establish the same for $N\geq 120k-240$. In fact we will establish in the next theorem, a stronger result, that every $N\geq 120k-240$ can be expressed as a sum of at most $k-1$, k-gonal numbers, for $k\geq 5$. We may restrict our attention to $k\geq 5$ since we have already established the theorem for $k=3$ and 4. To state the theorem it is convenient to set $m=k-2$, and define the n-th $(m+2)$-gonal number to be

$$p_n:=\frac{m}{2}(n^2-n)+n. \tag{7.3}$$

We have already established the theorem for triangle numbers and squares, and so we may assume that $m\geq 3$.

The tables of Pepin and Dickson establish that every positive integer $N<120m$ can be expressed as a sum of at most $m+2$, $(m+2)$-gonal numbers. We prove next a much stronger

result for $N \geq 120m$.

Theorem 7.4.1. *Let $m \geq 3$ and $N \geq 120m$. Then N is the sum of $m+1$ $(m+2)$-gonal numbers, at most four of which are different from 0 or 1*

Proof. Let $m \geq 3$ and N be a natural number with $N \geq 120m$. Let s_1 and s_2 be consecutive odd integers. The set of the numbers of the form $s + r$, where $s \in \{s_1, s_2\}$ and $r \in \{0, 1, \ldots, m-3\}$, contains a complete set of residue classes modulo m. Thus $N \equiv s + r \pmod{m}$ for some $s \in \{s_1, s_2\}$ and $r \in \{0, 1, \ldots, m-3\}$. Let

$$a := 2\left(\frac{N-s-r}{m}\right) + s = \left(1 - \frac{2}{m}\right)s + 2\left(\frac{N-r}{m}\right).$$

Then a is an odd integer, and $ma = 2N - 2s - 2r + sm$. This implies that $2N = ma + 2s + 2r - sm = m(a-s) + 2(s+r)$. Hence,

$$N = \frac{m}{2}(a-s) + s + r. \tag{7.4}$$

We make the following claims, which will allow us to apply Cauchy's Lemma.

Claim I. If $0 < s < \frac{2}{3} + \sqrt{8\frac{N}{m} - 8}$, then $s^2 < 4a$.

Claim II. If $s > \frac{1}{2} + \sqrt{6\frac{N}{m} - 3}$, then $s^2 + 2s + 4 > 3a$.

To prove the first claim we define the quadratic function,

$$f(s) := s^2 - 4a = s^2 - 4\left(1 - \frac{2}{m}\right)s - 8\left(\frac{N-r}{m}\right).$$

The graph of $f(s)$ is a parabola opening upward, and thus $f(s) < 0$, that is $s^2 < 4a$, provided that s is between its two zeros, which are given by

$$\begin{aligned}
&\frac{4(1-\frac{2}{m}) \pm \sqrt{16(1-\frac{2}{m})^2 + 32\left(\frac{N-r}{m}\right)}}{2} \\
&= \frac{4(1-\frac{2}{m}) \pm 4\sqrt{(1-\frac{2}{m})^2 + 2\left(\frac{N-r}{m}\right)}}{2} \\
&= 2\left(1-\frac{2}{m}\right) \pm 2\sqrt{\left(1-\frac{2}{m}\right)^2 + 2\left(\frac{N-r}{m}\right)}.
\end{aligned}$$

Now, since $m \geq 3$ we have $2(1-\frac{2}{m}) \geq \frac{2}{3}$ and since $m > r$,

$$2\sqrt{\left(1-\frac{2}{m}\right)^2 + 2\left(\frac{N-r}{m}\right)} > 2\sqrt{2\left(\frac{N-r}{m}\right)} > \sqrt{8\frac{N}{m} - 8}.$$

and thus if $0 < s < \frac{2}{3} + \sqrt{8\frac{N}{m} - 8}$ if follows that s is between the two zeros of $f(s)$, whence $f(s) < 0$.

To prove the second claim we define

$$g(s) := s^2 + 2s + 4 - 3a = s^2 + \left(-1 + \frac{6}{m}\right)s + 4 - 6\left(\frac{N-r}{m}\right),$$

whose positive zero is given by

$$\begin{aligned}
&= \frac{\left(1-\frac{6}{m}\right) + \sqrt{(1-\frac{6}{m})^2 - 4(-6\left(\frac{N-r}{m}\right) + 4)}}{2} \\
&< \frac{1}{2} + \frac{1}{2}\sqrt{24\left(\frac{N-r}{m}\right) - 15} = \frac{1}{2} + \sqrt{6\left(\frac{N-r}{m}\right) - \frac{15}{4}} \\
&< \frac{1}{2} + \sqrt{6\left(\frac{N}{m}\right) - 3},
\end{aligned}$$

for $m \geq 3$. Thus, for $s > \frac{1}{2} + \sqrt{6\frac{N}{m} - 3}$, $f(s) > 0$, that is, $s^2 + 2s + 4 > 3a$.

Now the length of the interval $I := (\frac{1}{2} + \sqrt{6\frac{N}{m} - 3}, \frac{2}{3} + \sqrt{8\frac{N}{m} - 8})$ is given by

$$\ell(I) = \frac{2}{3} - \frac{1}{2} + \sqrt{8\frac{N}{m} - 8} - \sqrt{6\frac{N}{m} - 3} \geq \frac{1}{6} + \sqrt{8\frac{N}{m} - 8} - \sqrt{6\frac{N}{m} - 3} > 4,$$

for $N \geq 120m$. It follows that I contains two consecutive odd positive integers s_1 and s_2. Let $s \in \{s_1, s_2\}$ be the odd integer satisfying $N \equiv s + r \pmod{m}$ with $r \in \{0, 1, \ldots, m-3\}$, so that we have (7.4).

Hence, there exist odd positive integers a and s that satisfy the condition $N = \frac{m}{2}(a - s) + s + r$ and the inequalities $s^2 < 4a$, $3a < s^2 + 2s + 4$. Cauchy's lemma implies that there exist t, u, v, w such that $a = t^2 + u^2 + v^2 + w^2$, and $s = t + u + v + w$. Thus, recalling our notation for the n-th $(m+2)$-gonal number in (7.3), we have

$$\begin{aligned} N &= \frac{m}{2}(a - s) + s + r \\ &= \left(\frac{m}{2}(t^2 - t) + t\right) + \left(\frac{m}{2}(u^2 - u) + u\right) + \left(\frac{m}{2}(v^2 - v) + v\right) + \left(\frac{m}{2}(w^2 - w) + t\right) + r \\ &= p_t + p_u + p_v + p_w + r, \end{aligned}$$

a sum of four $(m+2)$-gonal numbers and $m - 3$ zeros or ones, completing the proof. □

7.5 Related Results

Lebesgue and Realis 1872, 1873 proved that every positive integer is a sum of two squares and one triangle number, and also that every positive integer is a sum of two triangle numbers and one square. Legendre 1830 proved that for any k, every sufficiently large integer is a sum of five k-gonal numbers one of which is either 0 or 1.

Chapter 8

Conclusion

Polygonal numbers has been a topic of interest in mathematics since the ancient time of the Pythagoreans. Fermat and Cauchy with their remarkable theorem, the Polygonal Number Theorem, pioneered modern work on polygonal numbers. Later Leonard Euler who developed a special interest in these numbers, among other findings related to polygonal numbers, came up with an explicit formula for triangular numbers that are also perfect numbers. These numbers (polygonal numbers) have been of great use in number theory and other branches of mathematics as they relate to the formulation of different kinds of theorems, computation of probabilities, etc. In practice, polygonal numbers have played a vital role in counting, and computer programming as they are applied to numbering iterations of some computer programming loops. The paper began by giving a thorough definition of polygonal numbers. It discussed the basic polygonal numbers including triangular numbers, and square numbers and how these numbers are related. The paper further explores how triangular numbers are related to Pascal's triangle. It also discusses sums of squares in their respective chapters, as well as deducing and proving Lagrange's 4-squares theorem. In order to have a good understanding of what polygonal numbers are, the paper presents the concept of polygonal numbers focusing and analyzing some of their properties, facts and corresponding theorems with well elaborated proofs. Tables and figures are included for the illustration of polygonal numbers. All this work and an important lemma of Cauchy included in the paper, lay a

concrete foundation for the proposition and proof of the main theorem in our discussion of polygonal numbers, the Cauchy-Fermat Polygonal Number Theorem, which came in the last chapter.

Appendix A

Quadratic Residues and Quadratic Reciprocity

Definition A.0.1. i) Let p be a prime and a an integer with $p \nmid a$. Then a is called a quadratic residue $\pmod p$ if $a \equiv x^2 \pmod p$ for some integer x. Otherwise a is called a quadratic non-residue $\pmod p$.

ii) Let p be an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be 1 or -1 according as a is or is not a quadratic residue $\pmod p$.

Theorem A.0.1. *Let p be an odd prime and $a, b \in \mathbb{Z}$ with $p \nmid ab$. Then*

i) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$.

ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

iii) If $a \equiv b \pmod p$ *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

iv) $\left(\frac{a^2}{p}\right) = 1$.

Corollary A.0.1. *For any odd prime p,*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4; \\ -1, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. Immediate from part (i) of the preceding theorem. □

Theorem A.0.2. *For any odd prime p,*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod 8, \\ -1, & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

Theorem A.0.3. *Law of Quadratic Reciprocity. For any odd primes p, q, $(\frac{p}{q}) = (\frac{q}{p})$ unless $p \equiv q \equiv 3 \pmod 4$, in which case $(\frac{p}{q}) = -(\frac{q}{p})$. Equivalently,*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Appendix B

Geometry of Numbers

Definition B.0.2. Let $v_1, \ldots, v_m$ be a set of $m \leq n$ linearly independent (over $\mathbb{R}$) vectors in $\mathbb{R}^n$.

i) The set of vectors

$$\mathcal{L} = \left\{ \sum_{i=1}^{m} \lambda_i v_i : \lambda_i \in \mathbb{Z} \right\} = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m.$$

is called an m-dimensional lattice in $\mathbb{R}^n$, generated by $v_1, \ldots, v_m$.

ii) If $m = n$ then $\mathcal{L}$ is called a full lattice.

iii) The set $\{v_1, \ldots, v_m\}$ is called a basis for $\mathcal{L}$.

Note B.0.1. i) If $A = [v_1, v_2, \ldots, v_m]$ is the $n \times m$ matrix whose columns are the vectors v_i, then $\mathcal{L} = A\mathbb{Z}^m$, the image of $\mathbb{Z}^m$ under matrix multiplication by A.

ii) An m-dimensional lattice is a free $\mathbb{Z}$-module of rank m.

iii) If $\{v_1, \ldots, v_m\}$, $\{w_1, \ldots, w_m\}$ are two bases for $\mathcal{L}$, then there exists an invertible $m \times m$ matrix U over $\mathbb{Z}$ with $w_i = \sum_{j=1}^{m} u_{ij} v_j$, $1 \leq i \leq m$.

Definition B.0.3. Suppose that $\mathcal{L}$ is a full lattice with basis $v_1, \ldots, v_n$.

i) The set of points,

$$\mathcal{P} = \mathcal{P}(v_1, \ldots, v_n) = \left\{ \sum_{i=1}^{n} \lambda_i v_i : 0 \leq \lambda_i \leq 1 \right\},$$

is called the fundamental parallelepiped for $\mathcal{L}$ associated with the basis $\{v_1, \ldots, v_n\}$.

ii) The volume of $\mathcal{L}$, denoted $\Delta(\mathcal{L})$, is the volume of any fundamental parallelepiped associated with $\mathcal{L}$.

Note B.0.2. i) If $\mathcal{L} = A\mathbb{Z}^n$, then $\Delta(\mathcal{L}) = |det(A)|$.

ii) The volume of $\mathcal{L}$ does not depend on the choice of basis for $\mathcal{L}$.

B.1 Minkowski's Fundamental Theorem

Definition B.1.1. i) A set of points S in $\mathbb{R}^n$ is said to be symmetric about the origin if $x \in S$ implies $-x \in S$.

ii) A set of points S in $\mathbb{R}^n$ is called convex if whenever $u, v \in S$ and $\lambda \in \mathbb{R}$ with $0 \leq \lambda \leq 1$, then $\lambda u + (1 - \lambda)v \in S$.

Theorem B.1.1. *Minkowski. Let $\mathcal{L}$ be a full lattice in $\mathbb{R}^n$ of volume Δ and R be a convex subset of $\mathbb{R}^n$ symmetric about the origin.*

i) If $vol(R) > 2^n\Delta$, then R contains a nonzero point in $\mathcal{L}$.

ii) If $vol(R) = 2^n\Delta$ and R is closed, then R contains a nonzero point in $\mathcal{L}$.

Appendix C

Legendre's Equation

The Legendre equation is

$$ax^2 + by^2 - cz^2 = 0, \tag{C.1}$$

where a, b and c are positive integers. The equation is said to be in normal form if a, b, c are square-free and pairwise relatively prime. It is not hard to show that any Legendre equation can be reduced to one in normal form. Clearly, if (C.1) has a solution, then it has a primitive solution, that is one with $gcd(x, y, z) = 1$. If the equation is in normal form and has a primitive integer solution x, y, z, then

$$gcd(a, yz) = gcd(b, xz) = gcd(c, yz) = 1,$$

and we have

$$ax^2 + by^2 - cz^2 \equiv 0 \pmod{abc}, \tag{C.2}$$

or equivalently,

$$\begin{aligned} by^2 &\equiv cz^2 \pmod{a}, \\ ax^2 &\equiv cz^2 \pmod{b}, \\ ax^2 &\equiv -by^2 \pmod{c}. \end{aligned} \tag{C.3}$$

Thus, bc is a square $\pmod{a}$, ac is a square $\pmod{b}$ and $-ab$ is a square $\pmod{c}$. This proves one direction of Legendre's Theorem.

Theorem C.0.2. *Legendre. If* (C.1) *is in normal form, then it has a nonzero integer solution if and only if* bc, ac *and* $-ab$ *are quadratic residues modulo* a, b *and* c *respectively.*

Bibliography

[1] A. Cauchy, *Démonstration du théorème général de Fermat sur les nombres polygones, Mém. Sci. Math. Phys. Inst. France* (1) 14 (1813-15), 177-220 = Oeuvres (2), vol. 6, 320-353.

[2] P. L. Clark, *Number Theory: A Contemporary Introduction*. Online book from http://math.uga.edu/ pete/4400FULL.pdf.

[3] L. E. Dickson, *All positive integers are sums of values of a quadratic function of x*, Bull. Amer. Math. Soc. 33 (1927), 713-720.

[4] P. Fermat, quoted in T. L. Heath, *Diophantus of Alexandria*, Dover, New York, 1964, 188.

[5] C. F. Gauss, *Disquisitiones arithmeticae*, Yale Univ. Press, New Haven, Conn., and London, 1966.

[6] T. L. Heath, *Diophantus of Alexandria*, Dover, New York, 1964.

[7] J. L. Lagrange, *Démonstration d'un théorème d'arithmétique*, Nouveaux Mmoires de l'Acad. Royale des Sci. et Belles-L. de Berlin, 1770, pp. 123-133 = Oeuvres, vol. 3, 189-201.

[8] A.-M. Legendre, *Essai sur la thorie des nombres*, Paris, An VI (1797-1798), p. 202 and 398-399.

[9] A.-M. Legendre, *Théorie des nombres*, 3rd ed., vol. 2, 1830, 331-356.

[10] M. B. Nathanson, *A short proof of Cauchy's polygonal number theorem*, Proc. Amer. Math. Soc. 99 (1987), no. 1, 22-24.

[11] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An introduction to the theory of numbers, Fifth edition*, John Wiley and Sons, Inc., New York, 1991.

[12] T. Pepin, *Démonstration du théorème de Fermat sur les nombres polygones*, Atti Accad. Pont. Nuovi Lincei 46 (1892-93), 119-131.

[13] Polygonal number, (2015, November 4). In Wikipedia, The Free Encyclopedia. Retrieved 19:58, July 6, 2016, from https://en.wikipedia.org/w/index.php?title=Polygonal_number&oldid=689006720.