PELL'S EQUATIONS: A HANDSHAKE BETWEEN THE ANCIENT AND THE MODERN

by

K. McGilley Simons

Submitted in partial fulfillment of the
requirements for Departmental Honors in
the Department of Mathematics
Texas Christian University
Fort Worth, Texas

December 12, 2022

PELL'S EQUATIONS: A HANDSHAKE BETWEEN THE ANCIENT AND THE MODERN

Project Approved:

Supvervising Professor: Ze-Li Dou, PhD.
Department of Mathematics

Efton Park, PhD.
Department of Mathematics

Darren Middleton, PhD.
Department of Religion

Liran Ma, D.Sc.
Department of Computer Science

Abstract

This thesis is a comparative study between two approaches to a classical topic in number theory generally known as Pell's Equation. The equation has the general form

$$x^2 - Ny^2 = 1,$$

where N is a positive integer not equal to a perfect square. Only solutions in positive integers are sought. Because there are two unknowns, this is an example of an indeterminate equation; such equations are also called Diophantine equations, after Diophantus, the 3rd century Alexandrian mathematician whose masterpiece, *Arithmetica*, exerted an out-sized influence on the development of number theory.

The comparisons are temporal, geographical, as well as methodological. Diophantine equations have had a very long history. Though not written in the form we do now, the ancient Greeks, the Chinese, and the Indians were all interested in various genres of such equations. Each culture supplied its own motivation, however.

In the case of Pell's equations, the Indians, after mastering Diophantine equations of the linear type, considered them in the 7th century. Brahmagupta obtained foundational results concerning what he called "square-nature" problems, and singled out Pell's equations for the illustration of his general methods. Five centuries later, Bhaskaracharya completed the study of Pell's equation by establishing his *chakravala*, or cyclic method, which is totally general.

The Indian investigations of this topic, however, were entirely unknown to the Europeans for many centuries. When Fermat initiated his ground-breaking number theoretic studies in the 17th century, he thought he was recasting Diophantus's work on a grander foundation. Pell's Equation was a case study of the properties of what would become "units of algebraic integers"; but when Fermat challenged his contemporary peers to solve such equations, he probably imagined that no one without his insight into the bigger context would be successful.

William Brouncker, viscount and future President of the Royal Society, however, proved Fermat wrong by discovering a complete method within a few months. In retrospect, Lord Brouncker's discovery was an inadvertent illustration of how much the two seemingly distinct lines of research, the Indian and the European, had in common, when viewed methodologically. The *kuttaka*, or the pulverizer method, which both Brahmagupta and Bhaskaracharya relied upon, was in essence a variation of the familiar Euclidean Algorithm. Lord Brouncker, on the other hand, utilized the Euclidean Algorithm in an essential way as well; his study of what amounted to a study of continued fractions heavily depended on it. The main conclusion of this study is that the continued fractions expansion for the square root of N in the above equation is infinite but periodic. It was André Weil who first suggested that Brouncker's periodicity and Bhaskara's cyclicity are in fact closely related. This fact has been verified concretely in this thesis.

Moreover, this thesis also addresses the distinct styles in which the methods of solving Pell's equations are represented, in the Indian and Western literature respectively. The most glaring aspect of this stylistic distinction may be found in the specific techniques highlighted; while the Western style is to bring out the comprehensiveness and generality of the method, the Indian presentation emphasizes efficiency. The resulting apparent differences are so great that questions have been raised as to the completeness of the Indian method. (Chauvinism may also have played a role here.) It will be argued, though only briefly, that the differences are better understood as manifestations of cultural and philosophical influences at work.

"Comparative mathematics" is *not* a known academic discipline at the present time; rather, it is an emerging field of study. Only recently have the possibility and potential of systematic investigations of this type begun to be explored and explained. It is hoped that this thesis may be regarded as a sample specimen in support of such endeavors.

Acknowledgements

I would like to thank my family for sincerely supporting me in all my endeavors; without them, I would not be where I am today. A special thank you must go to my father, Monk Simons, for providing unwavering support, a fantastic sounding board, and a lot of laughs in every situation, and to my mother, Mona Simons, for showing me the highest example of perseverance, grace, and humility.

I also want to thank the TCU Department of Mathematics for their inspiration, thoughtful teaching, and wisdom, both inside and out of the classroom. The intentional encouragement I have received from so many members of the Math Department has meant the world to me, both as a student and as a lover of mathematics. I am especially appreciative of the TCU Math Club (and particularly of Dr. Emily Herzig and Dr. Igor Prokhorenkov for their guidance), an organization in which I have found fellow math aficionados and friends. I would also like to thank Dr. Ken Richardson for his help with technical questions about LaTeX in the writing of this thesis. Additionally, I am very grateful for my committee members for their careful reading and thoughtful comments to improve this project.

My utmost gratitude, however, is to Dr. Ze-Li Dou, my supervising professor. I wish to thank him for his encouragement and his willingness to share his wisdom in mathematics and in life. Words cannot express how grateful I am for all that he has done for me and for this thesis; without Dr. Dou, none of this would have been remotely possible.

Contents

1 Introduction

In 1657, Pierre de Fermat (1601 or 1607 – 1665)[1] wrote letters to his friend Bernard Frenicle de Bessy, his Dutch correspondent Frans van Schooten, and, through an intermediary, to the English mathematicians John Wallis and Viscount William Brouncker. In the letters, Fermat invited them—and indeed "all the others in Europe"—to solve some curious mathematical problems. The central questions are concerned with certain quadratic equations of the form

$$x^2 - Ny^2 = 1,$$

but only *nonzero integer* solutions are sought. To Wallis and Brouncker, he challenged them with the cases $N = 151$ and $N = 313$; but to his countryman Frenicle, he merely demanded answers for the cases $N = 61$ and $N = 109$, "so as not to give [him] too much trouble."[2]

Fermat was councilor at the provincial High Court of Judicature in Toulouse, but today he is almost exclusively remembered as an outstanding mathematician, and, in particular, "Father of Modern Number Theory." Fermat lived at the height of the period now known as the Scientific Revolution. By the time he wrote the letters, he had already made signal contributions in several major branches of mathematics, such as the soon-to-mature fields of analytic geometry, differential and integral calculus, and probability. In particular, his number-theoretic investigations had borne profound fruit, both in terms of results and, perhaps more important, methods. However, being "father" to a brand-new field of mathematics had its difficulties; Fermat had earlier tried to rouse the interest of eminent scientists of his day, such as Christiaan Huygens, but had met no success at all. Perhaps that was why he widened his net now. But if you think Fermat also lowered the standard in the challenge he issued, you would be wrong. It will be shown later in this thesis that his problems are indeed all solvable, but the least integer solutions to the "least" of these problems, the case $N = 61$, are given by

$$x = 1766319049, y = 226153980.$$

[1] Some authors have suggested that our Fermat, Pierre, had an older half-brother, Piere, who was born in 1601.
[2] We translated "peine" as "trouble." It is tempting to translate it as "so as to spare [him] of too much pain."

Hardly a trouble-free solution to obtain, if one does not have the know-how!

After a few months' hard work, Lord Brouncker, who in a couple of years would become the first President of the Royal Society of London for Improving Natural Knowledge, not only found solutions to Fermat's specific problems, but also announced a procedure for solving all equations of the same type. Although Fermat "willingly and joyfully acknowledge[d]" the correctness of the English method, he was clearly a little miffed; he would later complain, though not publicly, that the method still lacked a general proof, which was true.

However, it turns out that, unbeknownst to Fermat, I have begun this story *in medias res*—almost near the end, in fact. As the eminent mathematician André Weil, who was among the best number theorists in the 20th century, has remarked, "what would have been Fermat's astonishment if some missionary, just back from India, had told him that his problem had been successfully tackled there by native mathematicians almost six centuries earlier!"

Weil's remark refers to the work of the 12th century Indian mathematician Bhaskara II, also known as Bhaskaracharya.[3] It is quite possible to begin even sooner (as Weil knew well), as we shall soon see. Despite the known existence of (at least) two separate traditions, however, almost all published accounts of this topic in English adopt a Euro-centric viewpoint. While the Indian contributions are usually acknowledged, the treatment is usually cursory, if not downright curt. In addition, the directness and seemingly *ad hoc* nature of the Indian method could lead to questions about the depth of the Indian mathematicians' understanding of the topic—did they have a general theory, or were they merely reporting some numerical success on a few occasions? Such questions are reminiscent of Fermat's reaction to Brouncker's declaration of success. Unfortunately, though these questions are sometimes raised, they are almost never answered, whether this silence reflects ignorance, inattention, or chauvinism.

In this thesis, I shall attempt a comparative analysis of the "Indian" and "European" treatments of these equations, which are called Pell's Equations today.[4] Both methods of solving Pell's equation

[3]There was an Indian mathematician in the 7th century also named Bhaskara; our Bhaskara is called Bhaskara II for this reason. An alternative is to combine the name with an honorific: Bhaskaracharya – Bhaskara the master teacher.

[4]This term was coined by the Swiss mathematician Leonhard Euler, though the English mathematician John Pell had made no contribution of his own to the topic. An alternative term that has gained popularity recently is Fermat-Pell Equation. As we have already seen, this term is not accurate, either. For this reason, we have chosen to stay with the less cumbersome terminology.

will be described. Aspects of the methods that are in parallel and those that are distinct from each other will be marshaled and explained. Because of the emphasis on the "European" method in the general literature, however, this thesis will explain the "Indian" procedures in more detail. It follows from the technical discussions, I will argue, that the method of Bhaskaracharya was probably based on a mastery of the subject of Pell's equation at least as deep and complete as Brouncker's. The apparent dissimilarity between the presentations of the two methods, then, must have resulted from differences in style and emphasis rather than mathematical content. On the other hand, from the historical aspects of this thesis, I will also demonstrate that the Indian triumph was the culmination of a long, mostly algebraic tradition, while Fermat's "invention" of Pell equation was aimed at number theoretic developments whose full fruition still lay ahead of him. Pell's equation, therefore, provided a mathematical meeting ground of two (perhaps more) cultural as well as mathematical traditions, where a handshake of ideas was shared by the ancient and the modern, though the *dramatis personae* of this remarkable tale never even knew of the existence of one another.

In order to elucidate the parallelism as well as the distinctions between the Indian and European methods, and to facilitate experimentation by the reader to verify results and enhance comprehension, I have developed computer codes, written in Python, for the various algorithms required for solving Pell's equations. In particular, programs were created for the Euclidean Algorithm, continued fractions expansion for both rational and irrational real numbers. These, in turn, are embedded into solvers for Pell's equation to generate either the least integer solutions or all the solutions systematically (for there are always infinitely many), the Brahmagupta composition procedure for "square-nature" problems, and the cyclic (*chakravala*) method of Bhaskaracharya for solving Pell's equations. In addition, a separate program has been developed for the demonstration of the cyclicity of a "pure" version of the Bhaskaracharya method, which has never been recorded in Indian literature per se. This procedure aims to illustrate a suggestion of Weil, which asserts that the Indian method, as it is usually described in the literature, is a modification of an existing general method for the sake of speeding up the solving process; to which assertion we heartily agree. This implies that, far from being ignorant of the general theory, the Indian tradition had instead chosen to highlight an improvement that is more efficient, which is an amalgamation of methods developed by Brahmagupta and Bhaskaracharya. For this reason, Weil's assertion deserves to be much better

known. Incidentally, I believe that this last program has never been previously explicitly exhibited in the literature.

2 The European Approach

In Bertrand Russell's well-known *History of Western Philosophy*, we find the following interesting passage:

> The square root of 2, which is the first irrational to be discovered, was known to the early Pythagoreans, and ingenious methods of approximating to its value were discovered. The best was as follows:
>
> Form two columns of numbers, which we will call the a's and the b's. Each starts with 1. The next a, at each stage, is formed by adding the last a and b already obtained; the next b is formed by adding twice the previous a to the previous b. The first 6 pairs so obtained are
>
> $$(1,1),(2,3),(5,7),(12,17),(29,41),(70,99).$$
>
> In each pair, $2a^2 - b^2$ is 1 or -1. Thus b/a is nearly the square root of 2, and at each fresh step it gets nearer. For instance, the reader may satisfy himself that the square of $99/70$ is very nearly equal to $\sqrt{2}$.

The earliest record of the method here described, in the extant literature, is found in a work of Theon of Smyrna (2nd century CE)—the numbers generated by the algorithm are known as the "side and diagonal numbers." However, many learned scholars in addition to Bertrand Russell, such as Wilbur Knorr, are also of the opinion that the method dates back to a far earlier age. (Pythagoras lived in the 6th century BCE.) As Russell remarks, the pairs (b, a) satisfy equations

$$b^2 - 2a^2 = \pm 1.$$

Therefore, in effect, this may be seen as the first study of a Pell's equation. As we will see shortly, these pairs also give the "convergents" of the continued fractions expansion of $\sqrt{2}$. Consequently,

this procedure also suggests a possiblr relation between Pell's Equation $x^2 - Ny^2 = 1$ and the continued fractions expansion of $\sqrt{N}$.

This relation is precisely what we pursue in this section. We may, therefore, assert that, though the algebraic language would not be developed for more than a thousand years, the root idea of Pell's Equation, which was associated with the approximation of the square root of a natural number, had already been present with the early Pythagoreans in the sixth century BCE.

In this section, the material presented is standard in most number theory textbooks that discuss continued fractions. For this reason, we omit proofs of most of the theorems.

2.1 The Euclidean Algorithm

The basic idea behind Euclidean Algorithm is none other than that of division of two integers with remainder. The algorithm is indeed featured in Euclid's monumental *Elements* (Propositions 1 and 2 of Book VII), though knowledge of it surely predated Euclid (ca. 300 BCE), and was not confined in that general region. The ancient Chinese and Indian mathematicians, for example, were also aware of the procedure.

The Euclidean algorithm is an efficient way of finding the greatest common divisor (gcd) of two integers, say a and b. If $\gcd(a, b) = 1$, we say that a and b are *relatively prime*. In this setting of two integers, the algorithm is clearly finite. We illustrate this with one example below.

Example 1. Let $a = 78$, $b = 38$. We start by dividing 70 by 38 and recording the remainder; each following step is computed by dividing the previous divisor by the previous remainder. Therefore:

$$70 = 1 \cdot 38 + 32$$

$$38 = 1 \cdot 32 + 6$$

$$32 = 5 \cdot 6 + 2$$

$$6 = 3 \cdot 2 + 0$$

As described above, the last non-zero remainder in this procedure is the greatest common divisor of a and b. We can check that the gcd of 72 and 38 is indeed 2, the last non-zero remainder.

2.2 Finite Continued Fractions for Rational Numbers

The Euclidean Algorithm gives us the means to develop the continued fractions expansion for a rational number, i.e., a quotient of two integers. We illustrate this with the data in the previous example.

Example 2. Dividing each step in the previous example by the divisor, we obtain the folowing:

$$\begin{aligned}\frac{70}{38} &= 1 + \frac{32}{38}\\ \frac{38}{32} &= 1 + \frac{6}{32}\\ \frac{32}{6} &= 5 + \frac{2}{6}\\ \frac{6}{2} &= 3 + 0\end{aligned}$$

In each line, note that the remainder is the reciprocal of the beginning of the line following. Thus we can replace each of these remainders with the following expression:

$$\begin{aligned}\frac{70}{38} &= 1 + \frac{1}{38/32}\\ &= 1 + \cfrac{1}{1 + \cfrac{1}{32/6}}\\ &= 1 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{6/2}}}\\ &= 1 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{3}}}\end{aligned}$$

We denote finite continued fractions in the form $[a_0; a_1, a_2, \ldots, a_n]$. Thus $70/38 = [1; 1, 5, 3]$.

2.3 The Geometric Euclidean Algorithm and Infinite Continued Fractions

There is a geometric Euclidean Algorithm as well, which is less commonly known. Like the finite algorithm we have presented above, this is also featured in the *Elements* of Euclid, as Propositions 2 and 3 of Book X. In modern parlance, If we choose an arbitrary unit length, Euclid's geometric magnitudes may be understood as representing real numbers, which may or may not be rational. Thus, we may begin with $\alpha > \beta > 0$, and use β to "measure α"—that is, we subtract successive copies of β from α, until what remains is γ, where $0 \leq \gamma < \beta$. This done, the next step is to use γ to measure β if $\gamma > 0$, and so on.

It's easy to see that this procedure is entirely analogous to the "numeric" Euclidean Algorithm. If there is a common measure, δ, for α and β, then there are positive integers a and b, such that $\alpha = a\delta$ and $\beta = b\delta$. In that case, the procedure is essentially identical to the numerical Euclidean Algorithm for $a \div b$, and we say that α and β are commensurable (co-measurable); otherwise, the geometric Euclidean Algorithm will never terminate, and we say that α and β are incommensurable. It follows that α and β are commensurable if and only if α/β is a rational number. Put another way, α and β are incommensurable if and only if α/β is irrational.

We can use these simple observations to give a geometric proof that the so-called Golden Ratio—the Greeks called it the extreme and mean ratio—is irrational. Draw a regular pentagon. Its diagonals form a regular pentagram. It turns out to be the case that the ratio formed by the diagonal and the side of the regular pentagon is the Golden Ratio. If so, then the geometric way of stating the irrationality of the Golden Ratio is that the diagonal and the side of a regular pentagon are incommensurable. In order to demonstrate this, notice that the regular pentagram contains a smaller regular pentagon in the middle, for which we may again form a pentagram of diagonals. Now, in the larger pentagon, we can see that any two diagonals will cut each other into two segments. Moreover, it is easy to see that the longer segment is equal in length with the side of the larger pentagon, and the shorter segment is equal in length with the diagonal of the smaller pentagon. These facts, together with an obvious observation from similar isosceles triangles, imply that the large diagonal is to the large side as the large side to the smaller diagonal. This allows us to assert

that any two diagonals of the regular pentagon cut each other in the extreme and mean ratio, that is, the Golden Ratio. Finally, since the diagram of nested pentagons and pentagrams can be indefinitely produced due to similarity, we see that the geometric Euclidean Algorithm is interminable. Therefore, the Golden Ratio is irrational (i.e., the diagonal and the side of a regular pentagon are incommensurable). Written in the continued fractions notation, the Golden Ratio is given by

$$[1; 1, 1, 1, \dots] = [1; \overline{1}].$$

If we truncate a continued fraction as some point, a rational number will be produced. Such a rational number is referred to as a convergent of the continued fraction. In general, the convergents of a continued fraction may be generated recursively as the following theorem.

Theorem 1. Let $a_0, a_1, a_2, ..., a_n$ be real numbers with $a_1, a_2, ..., a_n$ positive. Let the sequences $p_0, p_1, ..., p_n$ and $q_0, q_1, ..., q_n$ be defined recursively by

$$\begin{aligned} p_0 &= a_0 & q_0 &= 1 \\ p_1 &= a_0 a_1 + 1 & q_1 &= a_1 \\ &\dots & &\dots \\ p_k &= a_k p_{k-1} + p_{k-2} & q_k &= a_k q_{k-1} + q_{k-2} \end{aligned}$$

for $k = 2, 3, ..., n$. Then the kth convergent $C_k = [a_0, a_1, a_2, ..., a_k]$ is given by

$$C_k = \frac{p_k}{q_k}.$$

The proof of this theorem will not be reproduced here, but the Python code for generating the convergents is included as part of Appendix A.

A very useful property of continued fractions is that every convergent of a continued fractions expansion of a real number is a *best rational approximation*. More precisely, if ρ is real number, and

$C_k = p_k/q_k$ is the k-th convergent of the continued fractions expansion of ρ, then

$$|\rho - C_k| = |\rho - p_k/q_k| \leq |\rho - m/n| \text{ for any } m, n \text{ with } |n| \leq |q_k|.$$

For example, it is known that the continued fractions expansion for π is

$$\pi = [3; 7, 15, 1, 292, \dots].$$

The fact that 15 is large implies that

$$[3; 7] = 3 + 1/7 = 22/7 \approx 3.14 = 314/100 = 157/50$$

is a very good approximation of π with a small denominator. This was first discovered by Archimedes of Syracuse in the 3rd century BCE. In the meantime, the fact that 292 is extraordinarily large implies that

$$[3; 7, 15, 1] = 355/113 \approx 3.141593 = 3141593/1000000$$

is an excellent approximation of π with such a small denominator. This was first established by the Chinese mathematician Zu Chongzhi in the 5th century CE.

2.4 Periodic Continued Fractions

A property of continued fractions especially important for the investigation of Pell's equations is that the expansion for $\sqrt{N}$, where N is a positive integer not equal to a perfect square, is infinite but *periodic*. In fact infinite periodicity of continued fractions expansion characterizes the so-called quadratic irrationality, which is an irrational number in the form of

$$\frac{a + b\sqrt{N}}{c}$$

where a, b, c, N are integers, and $N > 0$ is not a perfect square. For example, the Golden Ratio is equal to $(1+\sqrt{5})/2$, hence a quadratic irrationality. We have already seen that its quadratic fractions expansion is periodic. The general theorem regarding the periodicity of quadratic irrationalities was

first proved by Joseph-Louis Lagrange in the 18th century. Since the proof of this theorem is standard (but technical and long), it will not be reproduced here for the sake of space. We illustrate the occurrence of periodicity by an example below.

Example 3. For the continued fraction expansion of $\sqrt{3}$, we may begin by repeating the aforementioned steps for rational numbers; in this case, however, let $a = \sqrt{3}, b = 1$. Computing the steps yields the following:

$$\begin{aligned} \sqrt{3} &= 1 + (\sqrt{3} - 1) \\ \frac{1}{\sqrt{3}-1} &= \frac{\sqrt{3}+1}{2} = 1 + \frac{\sqrt{3}-1}{2} \\ \frac{2}{\sqrt{3}-1} &= \sqrt{3} + 1 = 2 + (\sqrt{3} - 1) \end{aligned}$$

Note that the remainder in the third line of the above algorithm is the same as that of the first line. Thus the algorithm begins to repeat at this step. Using these values, the continued fraction expansion is

$$[1; 1, 2, 1, 2, \dots] = [1; \overline{1, 2}]$$

Because $\sqrt{3} = [1; \overline{1, 2}]$, we say that the continued fraction of $\sqrt{3}$ has a period of length 2. We have seen before that $(1 + \sqrt{5})/2 = [1; \overline{1}]$ has a period of length 1. The reader can check that $\sqrt{2} = [1; \overline{2}]$ also has a period of length 1.

However, it is difficult to guess the length of a quadratic irrationality's period. For example, $\sqrt{51}$ has a period of length 2, but $\sqrt{61}$ has a period of length 11! The Python code for computing the continued fractions expansion of $\sqrt{N}$ for an arbitrary $N > 0$ that is not a perfect square is part of Appendix A.

2.5 Pell's Equation and Approximation of $\sqrt{N}$

We have already seen, in the introduction to this section, that the side-and-diagonal numbers of the square, which could be used to give arbitrarily close approximations to $\sqrt{2}$, happen to be solutions to the Pell-like equations

$$x^2 - 2y^2 = \pm 1.$$

Conversely, and more generally, if some pair of integers (x, y) solve one of the equations

$$x^2 - Ny^2 = \pm 1,$$

then we have

$$\left| \left(\frac{x}{y}\right)^2 - N \right| = \left| \frac{1}{y^2} \right|$$

This shows that, if we take $x, y > 0$, x/y would be a good approximation of $\sqrt{N}$. This is especially so if y is very large. From this point of view, we are not only interested in *a* solution for the equations, but in fact *all* solutions to them.

For the moment, however, the more pressing question is, do these equations, and in particular Pell's Equation, have nay non-zero solutions at all? Given the discussion so far, we are also interested in knowing whether or not the continued fractions expansion of $\sqrt{N}$, whose convergents also give good approximations of $\sqrt{N}$, may help us decide this question.

The answer, luckily, is affirmative in both cases. An insightful theorem of J. P. G. Lejeune Dirichlet (1805 – 1859) states that, given any irrational real number ρ, there are infinitely many integer pairs (x, y) such that

$$\left| \rho - \frac{x}{y} \right| < \frac{1}{y^2}.$$

This is a foundational theorem in the theory called *Diophantine Approximation.* As a consequence of this fact, one can further show that, if (x, y) is a pair of positive integers satisfying an equation of the form

$$x^2 - Ny^2 = m,$$

where m, N are integers, $N > 0$ is not a perfect square, and $|m| < \sqrt{N}$, then x/y is a convergent of the continued fractions expansion of $\sqrt{N}$.

It can be shown that these two theorems, when combined with the Brahmagupta Composition, which will be discussed in detail in the next section, are sufficient to establish the fact that every Pell's equation is not only solvable, but has infinitely many solutions. Furthermore, these same theorems can be used to prove the equivalence between the method of Lord Brouncker and a method that we believe belonged to Bhaskaracharya, as suggested by André Weil. [3, 11] Since the emphasis of

this project is not on the Diophantine approximation of algebraic numbers, however, we shall gloss over this part of the theory, but focus on a constructive method that exhibits all solutions to Pell's equations. This is, in fact, also faithful to history. The constructive part of the theory culminated in the work of Euler and Lagrange in the 1760s, while conscious and systematic study of Diophantine approximation arguably only began with Dirichlet's theorem just cited, which was first published in 1834. We remark, also, that for Pell's Equation, the constructive approach is more detailed and structurally complete.

Therefore, for the rest of this section, and again in the next section, we describe in detail how to obtain all the solutions, in positive integers, to an arbitrarily given Pell's Equation

$$x^2 - Ny^2 = 1,$$

where $N > 0$ is an integer that is not a perfect square. We insert here an incidental remark that, when N is a perfect square, the equation cannot afford a solution in positive integers, since, writing $N = n^2$, we have

$$x^2 - Ny^2 = (x + ny)(x - ny) = 1.$$

This is impossible because we require $y \neq 0$.

2.6 The Structural Theorems for the Solutions to Pell's Equations

In order to provide solutions to Pell's Equations via continued fractions, we state the following theorems; details can be found, for example, in [8].

Theorem 2. Let N be a positive integer that is not a square. Let p_k/q_k denote the kth convergent of the simple continued fraction of $\sqrt{N}$, $k = 1, 2, 3, ...$, and let n be the period length of this continued fraction. Then the following are true:

- When n is even, the positive solutions of the Diophantine equation $x^2 - Ny^2 = 1$ are $x = p_{jn-1}$, $j = 1, 2, 3, ...$, and the Diophantine equation $x^2 - Ny^2 = -1$ has no solutions.
- When n is odd, the positive solutions of $x^2 - Ny^2 = 1$ are $x = p_{2jn-1}$, $y = q_{2jn-1}$, $j = 1, 2, 3, ...$, and the solutions of $x^2 - Ny^2 = -1$ are $x = p_{(2j-1)n-1}$, $y = q_{(2j-1)n-1}$, $j = 1, 2, 3, ...$

Theorem 3. Let x_1, y_1 be the least positive solution of the Diophantine equation $x^2 - Ny^2 = 1$, where N is a positive integer that is not a square. Then all positive solutions x_k, y_k are given by

$$x_k + y_k\sqrt{N} = (x_1 + y_1\sqrt{N})^k$$

for $k = 1, 2, 3, ...$

These theorems allow us to utilize the periodicity of continued fractions to find all integer solutions to the equation $x^2 - Ny^2 = 1$.

2.7 Examples

The following examples illustrate the use of the previous theorems. We have included both even and odd period lengths to demonstrate the different results from Theorem 2. The answers to Fermat's challenge problems are included here as well.

Example 4. For $N = 23$ with the continued fraction expansion $[4; \overline{1, 3, 1, 8}]$, note that $n = 4$ is the length of the period of $\sqrt{N}$. By the previous theorem, since n is even, the positive solutions of the Diophantine equation $x^2 - 23y^2 = 1$ are $x = p_{4j-1}, y = q_{4j-1}$ for $j = 1, 2, 3, \ldots$ Thus the first positive solution ($j = 1$) is given by $x = p_3 = 24$, $y = q_3 = 5$, so

$$24^2 - 23 \cdot 5^2 = 1$$

is the first solution.

Consequently, all solutions are given by

$$x_k + y_k\sqrt{23} = (24 + 5\sqrt{23})^k$$

Thus the first solutions to the equation $x^2 - 23y^2 = 1$ are:

1. $x_1 = 24, y_1 = 5$
2. $x_2 = 1151, y_2 = 240$
3. $x_3 = 55224, y_3 = 11515$

4. $x_4 = 2649601, y_4 = 552480$

5. $x_5 = 127125624, y_5 = 26507525$

   ...

The data in this example are generated by the Python program included in Appendix A. Indeed, the output reads as follows.

```
Please input an integer N such that N is a positive integer that is not a square,
and x^2 - N*y^2 = 1 is the diophantine equation to be solved.

N:
23
Your equation input: x^2 - 23*y^2 = 1

Length of period: 4
The periodic portion is:
[1, 3, 1, 8]
The full continued fraction is:
[4, 1, 3, 1, 8]

# These are the kth convergents for the first 8 steps
k=0: 4/1 = 4.0
k=1: 5/1 = 5.0
k=2: 19/4 = 4.75
k=3: 24/5 = 4.8
k=4: 211/44 = 4.795454545454546
k=5: 235/49 = 4.795918367346939
k=6: 916/191 = 4.795811518324608
k=7: 1151/240 = 4.795833333333333
k=8: 10124/2111 = 4.7958313595452395
-----------
The least positive solution to the equation is:
x = 24, y = 5

All solutions are given by the equation:
x_k + y_k*sqrt(23) = [24 + 5*sqrt(23)]^k
for k = 1,2,3,...

Please input a specific integer k >= 2 to find the kth solution.

# Here the user inputs a value k to find the kth solution
k:
5
Your k input: 5
```

```
The specific solution for k = 5 is:
x_5 + y_5*sqrt(23) = 127125624 + 26507525*sqrt(23)
x = 127125624, y = 26507525
```

Example 5. For $N = 61$ with the continued fraction expansion $[7; \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}]$, note that $n = 11$ is the length of the period of $\sqrt{N}$. By the previous theorem, since n is odd, the positive solutions of the Diophantine equation $x^2 - 61y^2 = 1$ are $x = p_{22j-1}, y = q_{22j-1}$ for $j = 1, 2, 3, \ldots$ Thus the first positive solution ($j = 1$) is given by $x = p_{21} = 1766319049$, $y = q_{21} = 226153980$, so

$$1766319049^2 - 61 \cdot 226153980^2 = 1$$

is the first solution. Note that $C_{21} = p_{21}/q_{21} = 1766319049/226153980 \approx 7.810249675906654\cdots$; in fact, the error from the true value of $\sqrt{61}$ is a staggeringly minuscule 1.25×10^{-18}.

Then all solutions are given by

$$x_k + y_k\sqrt{61} = (1766319049 + 226153980\sqrt{61})^k$$

Thus the first solutions to the equation $x^2 - 61y^2 = 1$ are:

1. $x_1 = 1766319049, y_1 = 226153980$
2. $x_2 = 6239765965720528801, y_2 = 798920165762330040$
3. $x_3 = 22042834973108102061352541449, y_3 = 2822295814832482312327709940$

   ...

This example can similarly be illustrated by the output from the Python program included in Appendix A.

```
Please input an integer N such that N is a positive integer that is not a square,
and x^2 - N*y^2 = 1 is the diophantine equation to be solved.

N:
61
Your equation input: x^2 - 61*y^2 = 1
```

```
Length of period: 11
The periodic portion is:
[1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14]
The full continued fraction is:
[7, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14]

# These are the kth convergents for the first 22 steps
k=0: 7/1 = 7.0
k=1: 8/1 = 8.0
k=2: 39/5 = 7.8
k=3: 125/16 = 7.8125
k=4: 164/21 = 7.809523809523809
k=5: 453/58 = 7.810344827586207
k=6: 1070/137 = 7.810218978102189
k=7: 1523/195 = 7.81025641025641
k=8: 5639/722 = 7.810249307479224
k=9: 24079/3083 = 7.810249756730458
k=10: 29718/3805 = 7.810249671484888
k=11: 440131/56353 = 7.810249676148564
k=12: 469849/60158 = 7.810249675853585
k=13: 2319527/296985 = 7.810249675909557
k=14: 7428430/951113 = 7.810249675906017
k=15: 9747957/1248098 = 7.81024967590686
k=16: 26924344/3447309 = 7.810249675906627
k=17: 63596645/8142716 = 7.810249675906663
k=18: 90520989/11590025 = 7.810249675906652
k=19: 335159612/42912791 = 7.810249675906655
k=20: 1431159437/183241189 = 7.810249675906654
k=21: 1766319049/226153980 = 7.810249675906654
k=22: 26159626123/3349396909 = 7.810249675906654
-----------
The least positive solution to the equation is:
x = 1766319049, y = 226153980

All solutions are given by the equation:
x_k + y_k*sqrt(61) = [1766319049 + 226153980*sqrt(61)]^k
for k = 1,2,3,...

Please input a specific integer k >= 2 to find the kth solution.

# Here the user inputs a value k to find the kth solution
k:
2
Your k input: 2

The specific solution for k = 2 is:
x_2 + y_2*sqrt(61) = 6239765965720528801 + 79892016576233040*sqrt(61)
```

```
x = 6239765965720528801, y = 798920165762330040
```

Now we show the solutions to Fermat's other challenges, namely the cases of $N = 109, 151, 313$. It should come as no surprise that the least solutions for each of these cases are very large when compared to most other cases.

Example 6. For $N = 109$ with the continued fraction expansion $[10; \overline{2, 3, 1, 2, 4, 1, 6, 6, 1, 4, 2, 1, 3, 2, 20}]$, note that $n = 15$ is the length of the period of $\sqrt{N}$. By the previous theorem, since n is odd, the positive solutions of the Diophantine equation $x^2 - 109y^2 = 1$ are $x = p_{30j-1}, y = q_{30j-1}$ for $j = 1, 2, 3, \ldots$ Thus the first positive solution ($j = 1$) is given by $x = p_{29} = 158070671986249$, $y = q_{29} = 15140424455100$, so

$$158070671986249^2 - 109 \cdot 15140424455100^2 = 1$$

is the first solution.

Then all solutions are given by

$$x_k + y_k\sqrt{109} = (158070671986249 + 15140424455100\sqrt{109})^k.$$

Example 7. For $N = 151$ with the continued fraction expansion $[12; \overline{3, 2, 7, 1, 3, 4, 1, 1, 1, 11, 1, 1, 1, 4, 3, 1, 7, 2, 3, 24}]$, note that $n = 20$ is the length of the period of $\sqrt{N}$. By the previous theorem, since n is even, the positive solutions of the Diophantine equation $x^2 - 151y^2 = 1$ are $x = p_{20j-1}, y = q_{20j-1}$ for $j = 1, 2, 3, \ldots$ Thus the first positive solution ($j = 1$) is given by $x = p_{19} = 1728148040$, $y = q_{19} = 140634693$, so

$$1728148040^2 - 151 \cdot 140634693^2 = 1$$

is the first solution.

Example 8. For $N = 313$ with the continued fraction expansion $[17; \overline{1, 2, 4, 11, 1, 1, 3, 2, 2, 3, 1, 1, 11, 4, 2, 1, 34}]$, note that $n = 17$ is the length of the period of $\sqrt{N}$. By the previous theorem, since n is odd, the positive solutions of the Diophantine equation $x^2 - 313y^2 = 1$

are $x = p_{34j-1}, y = q_{34j-1}$ for $j = 1, 2, 3, \ldots$ Thus the first positive solution ($j = 1$) is given by $x = p_{33} = 32188120829134849$, $y = q_{33} = 1819380158564160$, so

$$32188120829134849^2 - 151 \cdot 1819380158564160^2 = 1$$

is the first solution.

For the previous three examples, note that we had to use the 29th, 19th, and 33rd convergents, respectively. This is a far cry from Example 4, in which we merely computed the first three convergents in order to find the first solution. Clearly Fermat had no intention to spare his contemporaries of any pain! For us, however, this also shows that, though Fermat never revealed his own method of solving to Pell's equation, he almost certainly did have a "complete theory," as he complained to Huygens that Brouncker did not.

3 The Indian Approach

The South Asian Subcontinent, which we will refer to as India for succinctness, is a land with a charmed history. It is connected enough with other regions of the world to allow cultural exchanges and knowledge transmission, and, at the same time, vast enough to allow the development of a distinct, rich, profound, and always magical culture of its own.

The mutual influences between the Indian culture and the neighboring cultures, the Greek, the Chinese, and later the Islamic, are widely acknowledged, but still insufficiently studied. The lack of extant documentation also poses problems. In the West, the exchanges between the Indian and the Greek and Islamic cultures have so far attracted more attention than those between India and China. [3] In this thesis, we will mostly focus on the topic of *indeterminate equations*.

Recall that a Pell's equation is an indeterminate equation, meaning that it may allow multiple, possibly an infinitude of, solutions. The Hellenistic mathematician Diophantus of Alexandria is so famous for his pioneering works that such indeterminate equations are often referred to as *Diophantine equations* in number theory today. We will follow this convention, but remark that most of the problems studied in his *Arithmetica* may be interpreted as quadratic equations.[5] In the meantime,

[5]However, only six of the thirteen books of the Arithmetica have survived.

India also had a long tradition in studying indeterminate equations. When the earliest surviving astronomical and mathematical compendium, the *Aryabhatiya*, by the eponymous Aryabhata, appeared around the year 500 CE, however, only *linear* equations were discussed. The quadratic equations would make their first appearance only in Brahmagupta's work, in the 7th century, and in a different region of northern India. Of course, systems of linear Diophantine equations—the source of the Chinese Remainder Theorem—had been studied in China since at least the 5th century CE.[6] In fact, linear Diophantine equations had been of interest to the Chinese mathematicians for the same reasons the Indian mathematicians were interested in them now—astronomy and calendars.

3.1 Aryabhata: Linear Diophantine Equations

The simplest of linear Diophantine equations, with two unknowns, are all we need for this thesis. They have the general form

$$ax + by = c,$$

where a, b, c are integers, and we seek integer solutions (x, y).

The key to solve the linear Diophantine equation is, once again, the Euclidean Algortithm already discussed in the previous section. The method introduced by Aryabhata is called the *kuttaka*, or the "pulverizer," and is a variation of the algorithm we have recorded in the previous section. Since our emphasis is on the quadratic equations, we will utilize the already established notation and results for the sake of space.

Theorem 4. Let a and b be integers with $d = \gcd(a, b)$. The equation $ax + by = c$ has no integral solutions if d does not divide c. On the other hand, if $d|c$, then there are infinitely many integral solutions. Additionally, if $x = x_0, y = y_0$ is a particular solution to the equation, then all solutions are give by

$$x = x_0 + \left(\frac{b}{d}\right) n,$$

$$y = y_0 - \left(\frac{a}{d}\right) n,$$

[6]The *Aryabhatiya* also contains other topics well known in ancient China but not in Egypt, Mesopotamia, or Greece, for example the methods of extracting the square and cubic roots, and an approximation of π, 3.1416. Significantly, Aryabhata reports this value without explanation while himself preferring the approximation $\sqrt{10}$. For this last, see the article at `https://mathshistory.st-andrews.ac.uk/Biographies/Aryabhata_I/` .

where n is any integer.

Theorem 5. Let a and b be positive integers. Then:

$$\gcd(a, b) = s_n a + t_n b$$

where s_n and t_n are the nth terms of the sequences defined recursively by:

$$s_0 = 1 \qquad t_0 = 0$$
$$s_1 = 0 \qquad t_1 = 1$$

and

$$s_j = s_{j-2} - q_{j-1} s_{j-1}$$
$$t_j = t_{j-2} - q_{j-1} s_{t-1}$$

for $j = 1, 2, 3, \ldots, n$ where the q_j are the quotients in the divisions of the Euclidean algorithm when used to find $\gcd(a, b)$.

Note that this theorem can be used to find linear combinations of a and b to find a solution to $ax + by = d$, where $d = \gcd(a, b)$.

Example 9. Let $a = 18, b = 50, c = 6$ such that $18x + 50y = 6$ is the equation to be solved. We begin by computing the steps to the Euclidean Algorithm for $a = 18, b = 50$:

$$50 = 2 \cdot 18 + 14$$
$$18 = 1 \cdot 14 + 4$$
$$14 = 3 \cdot 4 + 2$$
$$4 = 2 \cdot 2 + 0$$

Thus $\gcd(18, 50) = 2$. Using Theorem 5, we can then find the solution for when $d = \gcd(18, 50) = 2$:

$$2 = -11 \cdot 18 + 4 \cdot 50.$$

Multiplying by $d/c = 6/2 = 3$, we get

$$6 = -33 \cdot 18 + 12 \cdot 50$$

which gives us our first solution. Using Theorem 4, all solutions can then be given by

$$6 = 18(-33 + 25 \cdot n) + 50(12 - 9 \cdot n).$$

3.2 Brahmagupta: Square Nature Problems and the Composition Formula

Aryabhata had claimed that the purpose of his work was to restore the "astronomy of Brahman," apparently referring to the *Brahma-Siddhanta* (or *Brahman's Treatise*). Unfortunately, this work survives only in fragmentary form today. Likewise, a major work of the 7th century mathematician Brahmagupta, *Brahma-sphuta-siddhanta*, had the same purported aim, though Brahmagupta was very critical of Aryabhata's work! In fact, the title of the above treatise may be translated as *The Corrected Treatise of Brahman.*

Intellectual jostling notwithstanding, Brahmagupta did expound upon Aryabhata's pulverizer method of solving linear Diophantine equations and, from that, launched into an insightful investigation of certain homogeneous quadratic equations, which he called "square-nature" problems. Along the way, Brahmagupta also developed some algebraic identities of remarkable complexity—all this before the word "algebra" was coined!

We therefore consider equations of the form

$$x^2 = Ny^2 + m, \tag{1}$$

where $0 < N \in \mathbb{Z}$ is not a square and $m \in \mathbb{Z}$ could be positive or negative. We seek solutions

$(x, y) \in \mathbb{Z} \times \mathbb{Z}$, where $x, y \neq 0$. To denote the solutions for this equation, we will henceforth adopt the shorthand notation $(x, y; m)$, when the same N is understood in the discussion. Brahmagupta referred to equations of this type as "square-nature(d)" problems, where N is the "qualifier," m is the "additive," y is the "minor" root, and x is the "major" root.

From Brahmagupta we find the following composition rule:

$$[(x, y; m), (z, t; n)] \rightarrow (xz \pm Nyt, xt \pm yz; mn) \tag{2}$$

where the composition procedure ("production," *bhāvana*) is called "positive" if the terms are added and "negative" if not. It is also called "equal" if $(x, y) = (z, t)$ and "unequal" if not.
It can be easily seen that the composition rule corresponds to the following algebraic identity:

$$(x^2 - Ny^2)(z^2 - Nt^2) = (xz \pm Nyt)^2 - N(xt \pm yz)^2. \tag{3}$$

3.3 Brahmagupta: Solving Pell's Equation via Composition

The composition formula allowed Brahmagupta to solve Pell's equation

$$x^2 - Ny^2 = 1,$$

on condition that a solution of the form $(x, y; m)$ is known, where

$$m = \pm 1, \pm 2, \text{or} \pm 4.$$

In order to explain this method, we first make a few observations as follows:

Observation 1. From (2) we see see that, if a solution $(p, q; 1)$ is known, then the composition can give an indefinite number of solutions of the type $(x, y; m)$ from any of them. To see this, we simply compose $(p, q; 1)$ repeatedly with any solution $(x, y; m)$.

Observation 2. Composing $(x, y; m)$ with itself, we get some $(X, Y; m^2 = M)$. Thus we have

$$\left(\frac{X}{m}, \frac{Y}{m}; 1\right),$$

with $\frac{X}{m}, \frac{Y}{m} \in \mathbb{Q}$. So, in the case where they are *integers*, we have a solution for Pell's equation.

Observation 3. Similarly, if $(X, Y; \mu m^2)$ is a solution, then $(\frac{X}{m}, \frac{Y}{m}; \mu)$ is a solution. And if $\frac{X}{m}, \frac{Y}{m} \in \mathbb{Z}$, then it is an integer solution.

These observations allow us to explain Brahmagupta's rules for obtaining a solution for Pell's equation

$$x^2 - Ny^2 = 1$$

in the case of a known solution $(p, q; m)$, where $m = -1, m = \pm 2$, or $m = \pm 4$.

Case 1. $m = -1$. We compose $(p, q; m) = (p, q; -1)$ with itself, and obtain

$$(p^2 + Nq^2, 2pq; 1).$$

Case 2. $m = \pm 2$. We compose $(p, q; m) = (p, q; \pm 2)$ with itself and obtain

$$(p^2 + Nq^2, 2pq; 4).$$

Since $p^2 - Nq^2 = \pm 2$, we have that $p^2 + Nq^2 = 2Nq^2 \pm 2$, which implies that $2 \mid p^2 + Nq^2$. Therefore we have an integer solution

$$\left(\frac{p^2 + Nq^2}{2}, pq; 1\right).$$

Case 3. $m = \pm 4$, and suppose p is even in $(p, q; m)$. Then we have that $4 \mid p^2$. Since $p^2 - Nq^2 = \pm 4$, $Nq^2 = p^2 \pm 4$. Therefore $4 \mid Nq^2$.
Now the composition of $(p, q; m) = (p, q; \pm 4)$ with itself yields

$$(p^2 + Nq^2, 2pq; 16).$$

Since $4 \mid p^2 + Nq^2$, we have that $(\frac{p^2+Nq^2}{4}, \frac{pq}{2}; 1)$ is an integer solution.

Case 4. $m = \pm 4$, and suppose p is odd. We have seen that composing $(p, q; \pm 4)$ with itself gives

$$(p^2 + Nq^2, 2pq; 16).$$

Now we compose this solution with $(p, q; \pm 4)$ again. The result is

$$\begin{aligned}[p^3 + Npq^2 + N(2pq^2), 2p^2q + q(p^2 + Nq^2); \pm 64] \\ = [p^3 + 3Npq^2, 3p^2q + Nq^3; \pm 64].\end{aligned}$$

Since $p^2 - Nq^2 = \pm 4$, and since we assume p is odd, we know that Nq^2 is odd, which implies that N and q are both odd. Now

$$\begin{aligned}p^2 + 3Nq^2 &= (p^2 - Nq^2) + 4Nq^2 \\ &= 4Nq^2 \pm 4 \\ &= 4(Nq^2 \pm 1).\end{aligned}$$

Since Nq^2 is odd, $Nq^2 \pm 1$ is even, hence

$$\begin{aligned}8 \mid p^2 + 3Nq^2 &\implies 8 \mid p(p + 3Nq^2) \\ &\implies 8 \mid p^3 + 3Npq^2.\end{aligned}$$

Similarly, since $Nq^2 - p^2 = \pm 4$, we have

$$\begin{aligned}Nq^2 + 3p^2 &= (Nq^2 - p^2) + 4p^2 \\ &= 4p^2 \pm 4 \\ &= 4(p^2 \pm 1).\end{aligned}$$

But p is odd, and so $p^2 \pm 1$ is even. Therefore

$$\begin{aligned} 8 \mid Nq^2 + 3p^2 &\implies 8 \mid q(Nq^2 + 3p^2) \\ &\implies 8 \mid 3p^2q + Nq^3. \end{aligned}$$

We then conclude that

$$\left[\frac{1}{8}(p^3 + 3Npq^2), \frac{1}{8}(3p^2q + Nq^3); \pm 1\right]$$

is an integer solution.

Now, if the third entry of this solution is 1, we are done; if it is -1, then we compose it with itself and obtain

$$\left\{\frac{1}{64}[(p^3 + 3Npq^2)^2 + N(3p^2q + Nq^3)^2], 2 \cdot \frac{1}{64}(p^3 + 3Npq^2)(3p^2q + Nq^3); 1\right\},$$

which is an integer solution to Pell's equation.

The Python programs for these cases are included in a portion of Appendix B.

3.4 Bhaskaracharya: Solving Pell's Equation via the Cyclic Method

Bhaskaracharya's cyclic method can be described as follows:

Again, let N be fixed. Suppose we have a solution $(p, q; m)$, where m is "small" in some sense. We describe a way to find another triple

$$(p', q'; m'),$$

where m' is also "small." We show that our method eventually produces repeats, hence providing context for the name "cyclic."

First, we want to construct a triple $(x, y; M)$, where $M = m \cdot m'$. That is, M is a multiple of m. We also want m' to be small. Then, composing as we have done before, we obtain

$$(X, Y; m^2m').$$

Now, if X, Y are chosen such that $m \mid X$ and $m \mid Y$, then a new integer triple

$$\left(\frac{X}{m}, \frac{Y}{m}; m'\right) = (p', q'; m') \tag{4}$$

is found.

So we need to know how this can be achieved.

Let $y = 1$. Then $Ny^2 + M = X^2$ implies that $M = x^2 - Ny^2 = x^2 - N$.

We need to decide how to choose x. Because we have $y = 1$,

$$X = px + Nq, \qquad Y = p + qx. \tag{5}$$

Note that since $Nq^2 + m = p^2$, we may assume that $\gcd(m, q) = 1$ because, if not, we can write $d' = \gcd(m, q)$. Then $d' \mid p^2$. So we can let $d = \gcd(d', q)$. Then $d \mid p, d \mid q$, and $m = p^2 - Nq^2$ implies that $d^2 \mid m$. So we have

$$N\left(\frac{q}{d}\right)^2 + \frac{m}{d^2} = \left(\frac{p}{d}\right)^2 \implies \left(\frac{p}{d}, \frac{q}{d}; \frac{m}{d^2}\right)$$

is another integer triple featuring an even smaller m.

Therefore, we now assume that $\gcd(m, q) = 1$. This guarantees that the linear Diophantine equation

$$m\alpha - q\beta = p$$

is solvable, or

$$m\alpha = p + q\beta$$

is solvable. Therefore, if x is chosen as β among the solutions (α, β) for the equation above, then

$$Y = p + qx = m\alpha$$

is a multiple of m. (See (5).)

So far, we have decided to choose $y = 1$ and x such that $x = \beta$ for some solution of the equation $m\alpha = p + q\beta$. For any such choice, note that $m \mid p + qx$.

Now recall that the solution is $(x, y; M) = (x, 1; M)$. That is,

$$Ny^2 + M = N + M = x^2,$$

or

$$M = x^2 - N.$$

Therefore we have

$$q^2 M = q^2 x^2 - q^2 N. \tag{6}$$

On the other hand, $(p, q; m)$ is a solution. That is,

$$Nq^2 + m = p^2.$$

Thus

$$Nq^2 = p^2 - m. \tag{7}$$

Therefore,

$$\begin{aligned} q^2 M &= q^2 x^2 - q^2 N \\ &= q^2 x^2 - p^2 + m \\ &= (qx + p)(qx - p) + m \\ &= m \cdot \frac{qx + p}{m} \cdot (qx - p) + m \\ &= m \left[\frac{qx + p}{m} \cdot (qx - p) + 1 \right] \end{aligned}$$

Since $\gcd(m, q)=1$, we conclude that

$$m \mid M.$$

To summarize, recall that we let $y = 1$ and choose $x = \beta$ so that (α, β) is some solution of

$$m\alpha - q\beta = p,$$

which, in turn, is solvable since we may assume gcd(m, q)=1. Then $(x, y; M) = (x, 1; M)$ is a solution, where $Ny^2 + M = x^2$, or, since $y = 1$, $M = x^2 - N$. And we have shown that $m \mid M$.

The composition of $(p, q; m)$ and $(x, y; M)$ yields a triple

$$(X, Y; mM)$$

such that

$$NY^2 + mM = X^2,$$

where

$$X = px + Nq, \qquad Y = p + qx.$$

as defined above. Also,

$$Y = p + qx = p + q\beta = m\alpha,$$

since $m\alpha - q\beta = p$, so $m \mid Y$.

It follows that, since

$$X^2 = NY^2 + mM,$$

we have

$$m^2 \mid X^2 \implies m \mid X.$$

So, all the requirements we made in Equation (4) are satisfied. Therefore, for $m' = \frac{M}{m}$, we have that

$$\left(\frac{X}{m}, \frac{Y}{m}; \frac{Mm}{m^2}\right) = \left(\frac{X}{m}, \frac{Y}{m}; m'\right)$$

The only remaining desire is that m' needs to be small. To this end, we prove the following:
If $|m| < 2\sqrt{N}$, then we can make $|m'| < 2\sqrt{N}$ as well. Inductively, therefore, repeats will happen, since $2\sqrt{N}$ is finite.

We know that, within the congruence class of $x \mod m$, we can choose m such that

$$x < \sqrt{N} < x + |m|.$$

We know, therefore, that

$$\sqrt{N} - x > 0.$$

We show that, also, $\sqrt{N} + x > 0$. Since $\sqrt{N} < x + |m|$, we have $2\sqrt{N} < \sqrt{N} + x + |m|$. So, if $\sqrt{N} + x \leq 0$, then $2\sqrt{N} < |m|$, contradicting the assumption.

So we have $\sqrt{N} - x > 0$ and $\sqrt{N} + x > 0$. Therefore,

$$N - x^2 = (\sqrt{N} + x)(\sqrt{N} - x) > 0$$

But then

$$0 < N - x^2 = (\sqrt{N} + x)(\sqrt{N} - x) < (2\sqrt{N})(|m|) = 2|m|\sqrt{N}.$$

But $M = x^2 - N$, and $m' = M/m$. So

$$|m'| = \frac{|M|}{|m|} < \frac{2|m|\sqrt{N}}{|m|} = 2\sqrt{N}.$$

Finally, we show that it is always possible to begin with

$$(p, q; m)$$

with $m < 2\sqrt{N}$ for every given $N, N \in \mathbb{Z}, N > 0, N$ not a square.

Let $q = 1$. Then $p^2 = Nq^2 + m = N + m$, so $m = p^2 - N$. We choose p such that $|p^2 - N|$ is the smallest possible.

Let us examine the interval between k^2 and $(k+1)^2$.

$$(k+1)^2 - k^2 = 2k + 1.$$

Therefore, we have the following cases.

- For $k^2 + 1 \leq N \leq k^2 + k$, we have $p = k$.

  The largest $|m| = |p^2 - N| = |k^2 - N|$ is k.

  The smallest $\sqrt{N}$ is $\sqrt{k^2+1} > k$. Thus

$$|m| \leq k < \sqrt{k^2+1} \leq \sqrt{N} < 2\sqrt{N}.$$

- For $k^2 + k + 1 \leq N \leq k^2 + 2k$, we have $p = k + 1$.

  The largest $m = p^2 - N = (k+1)^2 - N = k$.

  The smallest $\sqrt{N}$ is $\sqrt{k^2+k+1} > k$. Thus

$$|m| \leq k < \sqrt{k^2+k+1} \leq \sqrt{N} < 2\sqrt{N}.$$

Example 10. Let $N = 61$. Bhaskara II begins with $x = 8$, $y = 1$. Then:

$$x^2 - 61y^2 = 3.$$

Bhaskara would then look for an integer β such that $3 \mid \beta + 8$ and $|\beta^2 - 61|$ is as small as possible. That is, you are solving the equation

$$3\alpha = \beta + 8.$$

Thus $\beta = 7$ is the answer. Then $\beta^2 - 61 = 7^2 - 61 = -12$. So our two solutions to the equation are:

$$8^2 - 61 \cdot 1^2 = 3 \implies (8, 1; 3),$$

$$7^2 - 61 \cdot 1^2 = -12 \implies (7, 1; -12).$$

Using Brahmagupta's composition formula, this yields:

$$[(8,1,;3),(7,1;-12)] \to (117,15;-36)$$

for the form $(x,y;m)$, of which x,y are guaranteed to be divisible by 3, and m is divisible by 3^2. After factoring this out, we obtain:

$$(39,5;-4) \implies x^2 - 61y^2 = -4$$

which can now be inputted into Brahmagupta's equation for solutions to Pell's equations. So the Brahmagupta formula above yields:

$$1766319049^2 - 61 \cdot 226153980^2 = 1.$$

Thus $x = 1766319049, y = 226153980$ is a solution to $x^2 - 61y^2 = 1$ by the cyclic method.

The output for the code as described in Appendix B is as follows:

```
Please input an integer N that is not a square such that x^2 - Ny^2 = 1
is the equation to be solved.

N:
61

Your equation input: x^2 - 61y^2 = 1

# Note that the following series of three values are of the form (x,y;m).
Finding first equation:
8 1 3
Finding second equation:
7 1 -12
Composing these equations:
117 15 -36
Simplify:
39 5 -4

Using Brahmagupta's solutions:
1766319049 226153980 1
```

```
Answer: 1766319049^2 - 61*226153980^2 = 1
```

Note that this method for solving the $N = 61$ is much quicker than the aforementioned European method via continued fractions.

Additionally, the fact that this leads to periodic behavior is similar to the work of Lagrange (Euler found similar results, but a bit later). [3] We omit the discussion here.

3.5 The Pure Cyclic Method Suggested by André Weil

The cyclic method without the use of Brahmagupta's "shortcuts" follows the logic of the aforementioned method with one caveat: when $m = \pm 1, \pm 2, \pm 4$, instead of terminating the method by plugging our values into Brahmagupta's formulas, we continue to iterate steps of the cyclic method.

We illustrate this cyclicity with two examples that should already be familiar.

Example 11. Let $N = 23$. We have included the output from the program in Appendix C to demonstrate this method.

```
Please input an integer N that is not a square such that x^2 - Ny^2 = 1
is the equation to be solved.

N:
23

Your equation input: x^2 - 23y^2 = 1

# These are the first solutions to the equation, as given by 5^2 - 23*1 = 2.
p: 5, q: 1, m: 2

# We find beta such that m*alpha - a*beta = p
alpha0: 3, beta0: 1
# We now find x such that x = beta = beta0 + mt,
#  where x < sqrt(N) < x + abs(m)
x: 3
# M is found as x^2 - N
M: -14
# The new X,Y,M values are determined by Brahmagupta's composition
X: 38, Y: 8, newM: -28
# The following pp,qq,mm are the previous X,Y,M values when simplified
```

```
pp: 19, qq: 4, mm: -7

# Since our m value is not equal to 1, we repeat.

alpha0: -5, beta0: 4
x: 4
M: -7
X: 168, Y: 35, newM: 49
pp: 24, qq: 5, mm: 1

# Here, our m value is 1. However, to show cyclicity, we repeat this process.

alpha0: 29, beta0: 1
x: 4
M: -7
X: 211, Y: 44, newM: -7
pp: 211, qq: 44, mm: -7

alpha0: -49, beta0: 3
x: 3
M: -14
X: 1645, Y: 343, newM: 98
pp: 235, qq: 49, mm: 2

alpha0: 142, beta0: 1
x: 3
M: -14
X: 1832, Y: 382, newM: -28
pp: 916, qq: 191, mm: -7

alpha0: -240, beta0: 4
x: 4
M: -7
X: 8057, Y: 1680, newM: 49
pp: 1151, qq: 240, mm: 1

The length of the period is: 4
```

Notice that our values of m began to repeat and, in fact, will repeat in this pattern for a period length of 4. This corresponds to the continued fraction expansion of $\sqrt{23} = [4; \overline{1, 3, 1, 8}]$, which also has a period length of 4!

Example 12. Let $N = 61$. Similar to the previous example, we have included the output from the program in Appendix C to demonstrate this method.

```
Please input an integer N that is not a square such that x^2 - Ny^2 = 1
is the equation to be solved.

N:
61

Your equation input: x^2 - 61y^2 = 1

# These are the first solutions to the equation, as given by 8^2 - 61*1 = 3.
p: 8, q: 1, m: 3

# We find beta such that m*alpha - a*beta = p
alpha0: 3, beta0: 1
# We now find x such that x = beta = beta0 + mt,
#  where x < sqrt(N) < abs(m)
x: 7
# M is found as x^2 - N
M: -12
# The new X,Y,M values are determined by Brahmagupta's composition
X: 117, Y: 15, newM: -36
# The following pp,qq,mm are the previous X,Y,M values when simplified
pp: 39, qq: 5, mm: -4

# Since our m value is not equal to 1, we repeat.

alpha0: -11, beta0: 1
x: 5
M: -36
X: 500, Y: 64, newM: 144
pp: 125, qq: 16, mm: 9

alpha0: 21, beta0: 4
x: 4
M: -45
X: 1476, Y: 189, newM: -405
pp: 164, qq: 21, mm: -5

alpha0: -37, beta0: 1
x: 6
M: -25
X: 2265, Y: 290, newM: 125
pp: 453, qq: 58, mm: 5

alpha0: 137, beta0: 4
x: 4
M: -45
X: 5350, Y: 685, newM: -225
pp: 1070, qq: 137, mm: -9
```

```
alpha0: -195, beta0: 5
x: 5
M: -36
X: 13707, Y: 1755, newM: 324
pp: 1523, qq: 195, mm: 4

alpha0: 527, beta0: 3
x: 7
M: -12
X: 22556, Y: 2888, newM: -48
pp: 5639, qq: 722, mm: -3

alpha0: -2361, beta0: 2
x: 5
M: -36
X: 72237, Y: 9249, newM: 108
pp: 24079, qq: 3083, mm: 12

alpha0: 3805, beta0: 7
x: 7
M: -12
X: 356616, Y: 45660, newM: -144
pp: 29718, qq: 3805, mm: -1

# Here, our m value is -1, so we could square the previous pp,qq,mm to find a solution;
#  however, to show cyclicity, we repeat this process.

alpha0: -33523, beta0: 1
x: 7
M: -12
X: 440131, Y: 56353, newM: 12
pp: 440131, qq: 56353, mm: 12

alpha0: 60158, beta0: 5
x: 5
M: -36
X: 5638188, Y: 721896, newM: -432
pp: 469849, qq: 60158, mm: -3

alpha0: -176669, beta0: 1
x: 7
M: -12
X: 6958581, Y: 890955, newM: 36
pp: 2319527, qq: 296985, mm: 4

alpha0: 654128, beta0: 1
x: 5
```

```
M: -36
X: 29713720, Y: 3804452, newM: -144
pp: 7428430, qq: 951113, mm: -9

alpha0: -1248098, beta0: 4
x: 4
M: -45
X: 87731613, Y: 11232882, newM: 405
pp: 9747957, qq: 1248098, mm: 5

alpha0: 2199211, beta0: 1
x: 6
M: -25
X: 134621720, Y: 17236545, newM: -125
pp: 26924344, qq: 3447309, mm: -5

alpha0: -8142716, beta0: 4
x: 4
M: -45
X: 317983225, Y: 40713580, newM: 225
pp: 63596645, qq: 8142716, mm: 9

alpha0: 11590025, beta0: 5
x: 5
M: -36
X: 814688901, Y: 104310225, newM: -324
pp: 90520989, qq: 11590025, mm: -4

alpha0: -31322766, beta0: 3
x: 7
M: -12
X: 1340638448, Y: 171651164, newM: 48
pp: 335159612, qq: 42912791, mm: 3

alpha0: 140328398, beta0: 2
x: 5
M: -36
X: 4293478311, Y: 549723567, newM: -108
pp: 1431159437, qq: 183241189, mm: -12

alpha0: -226153980, beta0: 7
x: 7
M: -12
X: 21195828588, Y: 2713847760, newM: 144
pp: 1766319049, qq: 226153980, mm: 1

The length of the period is: 11
```

Note that this solution is much longer than that of Section 3.4 when using Brahmagupta's "shortcut"; in fact, the length of this process is much more like that of the European method in Section 2.7.

4 Comparison and Conclusion

The comparative approach to the scholarly study in diverse disciplines, such as literature, fine arts, social sciences, and even religion, has by now had a fairly long history, and is widely adopted and accepted. In the fields of natural sciences, however, this is not so—comparative physics would have an odd ring in people's ears, and the word "comparative" in comparative botany would have a quite different meaning.

Mathematics occupies a unique place in the humanities/natural sciences divide. Philosophers of mathematics have long debated about the nature of mathematical objects and mathematical theorems in relation to the physical world. Are they abstractions of realizable things, or are they abstract and *independent* entities altogether?

A conscious and formal division of these two viewpoints is, of course, a product of the Western philosophical tradition, heavily influenced by the philosophical tenets of Plato and Aristotle—in fact, the just-mentioned positions are usually called Aristotelianism and Platonism, respectively. While Platonism became prevalent among Western mathematicians, most ancient practitioners of mathematics in the "non-Western" parts of the world tacitly (though perhaps naïvely) assumed an inherent connection between mathematics and the "real world." In his course on the history of mathematics, Ze-Li Dou has further argued that the attitude regarding the nature of mathematics had exerted great influence on the choice of mathematical problems, on the perception of their relative importance, on the methodology of problem solving, and on the (re)presentation of mathematical truth. It follows that studying mathematics comparatively is fully justified. [2]

4.1 Remarks on the European Method

The topic of Pell's Equation may be taken as an exemplar for comparative mathematics. Fermat's number-theoretic investigations that led to the topic had begun with his study of the *Arithmetica* of the 3rd century Alexandrian mathematician Diophantus. Ironically, *Arithmetica* is composed in

a style radically different from that of the far-famed earlier Alexandrian, Euclid. Unlike the *Elements*, the *Arithmetica* is a choppy and to-the-point collection of questions and answers. Moreover, Diophantus often contented himself with merely exhibiting a single solution for his indeterminate equations affording infinitely many solutions.

To Fermat, this must have been a welcome style, since it left open a wide space for imagination and a plethora of leads for possible discoveries. For instance, the famous Fermat's Last Theorem, only recently proved,[7] was originally a marginal note in just that book. In posing Pell's Equation, if we allow ourselves to use modern terminology, Fermat was pioneering the study of *quadratic forms*, that is, homogeneous quadratic polynomials in several variables. This was an ambitious and forward-looking program, anticipating the magisterial work of Carl Friedrich Gauss[8] and, moreover, the development of algebraic number theory in the 19th century. (See, for example, [6].) More precisely, here one inquires what rational integers are represented by the quadratic form $x^2 - Ny^2$, and the equation

$$x^2 - Ny^2 = 1,$$

then, addresses the *units of the ring of algebraic integers in the quadratic number field* $\mathbb{Q}(\sqrt{N})$. All very natural—though, of course, only so after the theory is complete. To be able to envision a grand, abstract theory right at the beginning of the investigation required, of course, genius of Fermat's caliber. However, at the same time, such an endeavor was entirely in keeping with the Platonic understanding of the nature as well as the purpose of mathematics.

From this point of view, Fermat's complaint, even after Lord Brouncker announced a full procedure for solving the equations, that the method still lacked a "full proof," was understandable. Though Fermat never published such a full proof himself, circumstantial evidence suggests that he might well have had one in his mind. In any case, what was eventually worked out by Euler and Lagrange had been well within Fermat's reach, though it took more than 100 years for it to appear in the literature. [2, 3]

[7] Andrew Wiles proved this theorem with some assistance from Richard Taylor, in 1993 – 1994.
[8] *Disquisitiones Arithmeticae*, 1801.

4.2 Remarks on the Indian Method

By contrast, the investigations of Brahmagupta on "square-nature" problems—in mathematical nature very like quadratic forms—may be seen as an extension of a long-standing Indian tradition of studying indeterminate equations. Indian mathematicians had very good reasons to be interested in linear Diophantine equations, because they were relevant in the study of astronomy, and, by extension, also useful in calendrical studies. In fact, even the title of his work explicitly states this, as we have mentioned earlier.

It is not clear whether or not Brahmagupta had applications in mind when he proposed his square-nature problems, and, if so, what the applications might be. Though Indian mathematics was more pragmatic than its Greek counterpart, it was clearly not a stagnant pool of rules-of-thumb; the Indian thinkers seemed never to fall into dogmatic slumbers. However, we do see that the techniques developed to obtain solutions of the square-nature problems were similar in kind to those for linear Diophantine equations. In both instances, the method was essentially one of transformation among equations of the same type, so that solutions to harder equations may be obtained through the knowledge of the easier ones. It is for this reason that we are tempted to say that the Indian approach had a traditional outlook and an algebraic nature, though the word *algebra* was not yet in place.[9]

Of course, the Indian method for solving Pell's Equations, as presented by Bhaskaracharya, does not exhibit a full proof, either. In fact, as we have seen, not even a full procedure is explained: whenever a shortcut is possible, it is invariably taken. This once again shows a reverence for tradition, but more can be said here. In the *Bija-ganita*, the work that contains his cyclic method, Bhaskaracharya states that the purposes of mathematical demonstrations, which he calls *upapatti*, are these two:

1. To remove confusion and doubts regarding the interpretation of mathematical results, and of their validity;

2. To obtain assent in the community of mathematicians.

Therefore, for Indian mathematicians like Bhaskaracharya, the presentation of mathematics,

[9]We note in passing that the "Arabic numerals" were "Hindu" in origin as well.

rather than needing to conform to certain pre-ordained format such as the Euclidean axiomatic approach, might well have had an element of performance in it, where nimbleness and brilliance, like the cream of *ghee* in milk, or like the *rasa* of a piece of ripe fruit or a fine *raga*, are not only acceptable, but valued and avidly sought—they are the very essence. It should not at all come as a surprise, then, that the method as presented is but the tip of the iceberg that comprises the total comprehension. The table, therefore, is turned—accusations of incompleteness or even ignorance, unless carefully *proven*, may instead be a reflection of ignorance on the accuser's part. [2, 3]

4.3 Coda

Although Pell's Equation provides a near-ideal topic for a comparative study of ancient Greek and Indian mathematics, its interest does not stop there. For example, a remarkable poem, attributed to the great Archimedes of Syracuse (3rd century BCE), poses a charming question on the number of cattle belonging to *Helios*, the Sun god. Archimedes, too, kept the solution hidden. It turns out that this *Cattle Problem* of Archimedes amounts to a Pell's Equation, and the least solution is greater than 10^{200000}.[10] Is that why Archimedes never revealed it? [2]

We may also partially motivate the study of algebraic numbers by raising a natural, but also "philosophical," question. We are all used to the distinction between the rational and irrational real numbers. We know, further, that the rational numbers are characterized by the fact that their decimal expansions are either finite or infinite but periodic. We have now just seen, however, that if we were to use the same criterion, but on the continued fractions expansions, the classification of real numbers would have been much different. This raises the question of what other "natural" classifications are possible. It turns out that this question has a rich answer because of algebraic number theory. [3]

These fascinating questions and, indeed, many more, are topics of exploration for another day.

[10] Incidentally, physicists tell is that the numbers atoms in the visible part of the Universe is less than 10^{100}.

Appendix

The following programs were developed in Python in order to demonstrate the aforementioned methods to solve Pell's Equations.

A Python Code for Modern Solutions

```
# Modern Solutions
#  Using Chapter 13 in book
import math

# Finds kth convergents
# Using Theorem 12.9
def findKthConv(alist):
    # Define p: p0 = a0, p1 = a0*a1 + 1
    # Define q: q0 = 1, q1 = a1
    if len(alist) > 1:
        p = [alist[0], alist[0]*alist[1] +1]
        q = [1, alist[1]]
        # Now define all kth convergents
        if len(alist) > 2:
            for k in range(2,len(alist)):
            # 2 times the list to account for the odd indices later
                # Now take a new variable mod len(alist) so that it fits in the indices
                kmod = k
                pk = alist[kmod]*p[kmod-1] + p[kmod-2]
                p += [pk]
                qk = alist[kmod]*q[kmod-1] + q[kmod-2]
                q += [qk]
        for i in range(len(p)):
            print('k='+str(i)+": "+str(p[i])+"/"+str(q[i])+" = "+str(p[i]/q[i]))
        print('-----------')
        return(p,q)
    else:
        return(alist,[1])


# Finds least positive solution to equation: x^2 - d*y^2 = 1
# Using Theorem 13.11 (p. 555)
def findFirstSoln(d,period,p,q):
    n = len(period)
    # If n is even
    if n%2 == 0:
        x1 = p[n-1]
```

```
        y1 = q[n-1]
    # If n is odd
    else:
        x1 = p[2*n - 1]
        y1 = q[2*n - 1]
    print("The least positive solution to the equation is:")
    print("x = "+str(x1)+", y = "+str(y1))
    print()
    findAllSoln(d,x1,y1)
    return(x1,y1)

# Finds all solutions
# Parameters:
# - d: the integer to take the sqrt of
# - x1, y1: lease posiitve solution of the diophantine equation
# Using Theorem 13.12 (p. 557)
def findAllSoln(d,x1,y1):
    # Using the equation:
    #   xk + yk*sqrt(d) = (x1 + y1*sqrt(d))^k
    strSoln = "x_k + y_k*sqrt("+str(d)+")"\
         +"= ["+str(x1)+" + "+str(y1)+"*sqrt("+str(d)+")]^k"
    print("All solutions are given by the equation: ")
    print(strSoln)
    print("for k = 1,2,3,...")
    print()

# Finds the solution xk,yk for a given k
def findSpecSoln(d,x1,y1,k):
    # Using the equation:
    #   xk + yk*sqrt(d) = (x1 + y1*sqrt(d))^k
    coeffs = []
    xexp = []
    yexp = []
    for i in range(k+1):
        coeffs += [math.comb(k,i)]
        # comb(k,i) is "k choose i" -- part of the math package
        xexp += [k-i] # exponents go from k to 0
        yexp += [i] # exponents go from 0 to k
    # Deal with x and y values first
    xyvals = []
    for index in range(k+1):
        xy = coeffs[index]*(x1**(xexp[index])*(y1**(yexp[index])))
        # xy = coeff*(x1^xexp)*(y1^yexp)
        xyvals += [xy]
    # Now the square root (of d) values
    dvals = []
    for di in range(k+1):
        if di%2 == 0: # If it's an even index, the answer will be an integer
```

```
            deven = int(d**(di/2)) # answer is d^(index/2)
            dsq = 0 # no square root part
        else: # If it's an odd index
            # Deal with even part first
            deven = int(d**((di-1)/2)) # if di=1, this yields 1
            dsq = 1 # a single square root part
        dvals += [[deven,dsq]]
    # Multiply d values by the y values
    dxyvals = []
    for i in range(k+1):
        if i%2==0: # If even, no square roots
            dxy = xyvals[i]*dvals[i][0]
            dxyvals += [[dxy,0]] # 0 because no square root
        else: # If odd, has a square root
            dxy = xyvals[i]*dvals[i][0]
            dxyvals += [[dxy,1]] # 1 because has square root multiplied
    # Add all like terms together
    intpart = 0
    sqpart = 0
    for j in range(k+1):
        if j%2==0: # No square roots
            intpart += int(dxyvals[j][0])
        else: # Has square roots
            sqpart += int(dxyvals[j][0])

    return(intpart,sqpart)


print("Please input an integer N such that N is a positive integer that "\
      "is not a square, and x^2 - N*y^2 = 1 is the diophantine equation to be solved.")
print()
print("N: ")
in_d = input()
sqrtd = math.sqrt(int(in_d))
# Checks if d is positive and not a square
if int(in_d)>0 and (sqrtd - int(sqrtd))!=0:
    print("Your equation input: x^2 - "+in_d+"*y^2 = 1")
else:
    print("Please enter a positive integer that is not a square.")
print()

dlist = [int(in_d),1,0,1]
avals = []
alphavals = []
arr = findExpansion(dlist,avals,alphavals)
alist = arr[0]
alphalist = arr[1]
period = arr[2]
```

```
# Create a new list with alist and the following period,
#   minus the first repeat at the end of alist
# Example: n=90
#  alist = [9,2,18,2], period = [2,18], alistdub = [9,2,18,2,18]
alistdub = alist[:-1]+period

pqarr = findKthConv(alistdub)
xyarr = findFirstSoln(in_d,period,pqarr[0],pqarr[1])

print("Please input a specific integer k >= 2 to find the kth solution.")
print()
print("k: ")
in_k = input()
if int(in_k)>1:
    print("Your k input: "+str(int(in_k)))
else:
    print("Please enter a positive integer greater than 2.")
print()

intpart,sqpart = findSpecSoln(int(in_d),xyarr[0],xyarr[1],int(in_k))

print("The specific solution for k = "+str(int(in_k))+" is:")
specSoln = "x_"+str(int(in_k))+" + y_"+str(int(in_k))+"*sqrt("+str(int(in_d))+") = "
specSoln += str(intpart)+" + "+str(sqpart)+"*sqrt("+str(int(in_d))+")"
print(specSoln)
print("x = "+str(intpart)+", y = "+str(sqpart))
print("This yields: "+str(int(intpart**2 - int(in_d)*(sqpart**2))))
print()
print("The first 10 solutions for this equation are:")
for sol in range(10):
    intsol,sqsol = findSpecSoln(int(in_d),xyarr[0],xyarr[1],sol+1)
    print("x = "+str(intsol)+", y = "+str(sqsol))
    print()
```

B Python Code for Cyclic Method

```
# Cyclic Method
import math

def composition(x,y,m,z,t,n,N):
    a1 = x*z + N*y*t
    a2 = x*t + y*z
    a3 = m*n
    return (a1,a2,a3)
```

```
def brahmaSoln(x,y,m,N):

    if m==1:
        return (x,y,m)

    if m==-1:
        # Compose it with itself
        x1,y1,m1 = composition(x,y,m,x,y,m,N)
        return (x1,y1,m1)

    if m==2 or m==-2:
        # Compose it with itself
        x2,y2,m2 = composition(x,y,m,x,y,m,N)
        # Now divide by 2 and 2^2
        simp2 = simplify(x2,y2,m2,2)
        return simp2

    if m==-4 or m ==4:

        if x%2==0: # if the x value is even
            # Compose with itself
            x4,y4,m4 = composition(x,y,m,x,y,m,N)
            # Now divide by 4 and 4^2
            simp4 = simplify(x4,y4,m4,4)
            return simp4

        else: # if the x value is odd
            # Compose with itself
            x4_1,y4_1,m4_1 = composition(x,y,m,x,y,m,N)
            # Compose again
            x4_2,y4_2,m4_2 = composition(x,y,m,x4_1,y4_1,m4_1,N)
            # Now divide by 8 and 8^2
            x4_3,y4_3,m4_3 = simplify(x4_2,y4_2,m4_2,8)

            # Check if m4_3 = -1 or 1
            if m4_3==1:
                return (x4_3,y4_3,m4_3)
            else: # if m4_3 = -1
                # Compose with itself again
                x4_4,y4_4,m4_4 = composition(x4_3,y4_3,m4_3,x4_3,y4_3,m4_3,N)
                return (x4_4,y4_4,m4_4)

    else:
        return(0,0,0)


# Finds first equation, where y=1 and x is chosen
#    such that x^2 is closest to N
```

```
# Returns (x,1,m), where m is the computed solution
def firstEq(N):
    i = 1
    solns = [1,2] # default
    for i in range(N): # arbitrary, can't be larger than N
        if (i+1)**2 > N:
            # if (i+1)^2 is the first to be larger than N, then
            #   i^2 is the largest below N
            solns = [i,i+1]
            break
    # Now find which is closer
    x1 = abs(solns[0]**2 - N)
    x2 = abs(solns[1]**2 - N)
    if (x1 <= x2):
        m = solns[0]**2 - N
        return (solns[0],1,m)
    else:
        m = solns[1]**2 - N
        return (solns[1],1,m)

# Finds second equation:
# - Want beta such that m divides beta + x
# - Want abs(beta^2 - N) as small as possible
# - y is still 1
def secondEq(x,y,m,N):
    betas=[]
    # Find all betas that satisfy y*beta + x = m*alpha
    for beta in range(N):
        if (x+y*beta)%m==0:
            betas += [beta]

    x=0 #default
    for t in range(2*N):
        beta = betas[0] + abs(m)*t
        if beta < math.sqrt(N) and (beta + abs(m)) > math.sqrt(N):
            x = beta

    # Now find m value
    m = x**2 - N
    return (x,1,m)


# For (x,y;M), x and y are divisible by m,
#   and M is divisible by m^2
# NOTE: m is from the first equation!
def simplify(x,y,M,m):
    xsol = int(abs(x/m))
    ysol = int(abs(y/m))
```

```
    msol = int(M/(m**2))
    return (xsol,ysol,msol)

print("Please input an integer N that is not a square such that"\
      " x^2 - Ny^2 = 1 is the equation to be solved.")
print()
print("N: ")
in_N = input()
N = int(in_N)
print()

# Check if N is a square
if math.sqrt(N).is_integer():
    print('Please input an integer N such that N is not a square.')

else:
    print("Your equation input: x^2 - "+str(N)+"y^2 = 1")
    print()

    # First equation
    x1,y1,m1 = firstEq(N)
    print('Finding first equation:')
    print(x1,y1,m1)
    # Second equation
    x2,y2,m2 = secondEq(x1,1,m1,N)
    print('Finding second equation:')
    print(x2,y2,m2)
    # Compose two equations
    xc,yc,Mc = composition(x1,y1,m1,x2,y2,m2,N)
    print('Composing these equations:')
    print(xc,yc,Mc)
    # Simplify
    xs,ys,ms = simplify(xc,yc,Mc,m1)
    print('Simplify:')
    print(xs,ys,ms)
    print()


    while abs(ms)!=1 and abs(ms)!=2 and abs(ms)!=4:
        print('Reiterating second equation:')
        xs2,ys2,ms2 = secondEq(xs,ys,ms,N)
        print(xs2,ys2,ms2)
        print('Composing these equations:')
        xsc,ysc,Msc = composition(xs,ys,ms,xs2,ys2,ms2,N)
        print(xsc,ysc,Msc)
        print('Simplify:')
        xss,yss,mss = simplify(xsc,ysc,Msc,ms)
        print(xss,yss,mss)
```

```
        xs = xss
        ys = yss
        ms = mss
        print()

    x,y,m = brahmaSoln(xs,ys,ms,N)
    print('Using Brahmagupta\'s solutions:')
    print(x,y,m)
    print()
    print('Answer: '+str(x)+'^2 - '+str(N)+'*'+str(y)+'^2 = '+str(m))
```

C Python Code for Cyclicity

```
# SHOW CYCLICITY
import math
#-------------PREVIOUS PROGRAMS-----------------
# Finds GCD (simplified from previous program)
def findGCD(a,b):
    answer = 1
    if a==0:
        # if a=0, the last nonzero remainder is b
        answer = b
        return answer
    if b==0:
        # if b=0, the last nonzero remainder is a
        answer = a
        return answer
    else:
        div = int(a/b)
        rem = a%b # remainder
        return(findGCD(b,rem))
        # recursively runs with b and remainder

# Finds first equation, where y=1 and x is chosen
#    such that x^2 is closest to N
# Returns (x,1,m), where m is the computed solution
def firstEq(N):
    i = 1
    solns = [1,2] # default
    for i in range(N): # arbitrary, can't be larger than N
        if (i+1)**2 > N:
            # if (i+1)^2 is the first to be larger than N, then
            #   i^2 is the largest below N
            solns = [i,i+1]
```

```
            break
    # Now find which is closer
    x1 = abs(solns[0]**2 - N)
    x2 = abs(solns[1]**2 - N)
    if (x1 <= x2):
        m = solns[0]**2 - N
        return (solns[0],1,m)
    else:
        m = solns[1]**2 - N
        return (solns[1],1,m)
#-----------------------------------------------------

# To count period length
counter = 0
repeat = False

def findCyc(p,q,m,N,counter,repeat):

    # To count period length
    if repeat==True:
        counter += 1

    # Consider m*alpha - a*beta = p
    # Use linear Diophantine code to find a solution (alpha_0, beta_0)
    alpha0,beta0 = findSoln(m,q,p)
    print()
    print('alpha0: '+str(alpha0)+', beta0: '+str(beta0))

    # Now want to find x = beta = beta0 + mt,
    #  such that x < sqrt(N) < x + abs(m)
    x=0 # default
    for t in range(N+1):
        beta = beta0 + abs(m)*t
        if beta < math.sqrt(N) and (beta + abs(m)) > math.sqrt(N):
            x = beta
    print('x: '+str(x))

    # Now compute new M value
    M = x**2 - N
    print('M: '+str(M))

    # Brahmagupta composition
    X = p*x + N*q
    Y = p + q*x
    newM = m*M
    print('X: '+str(X)+', Y: '+str(Y)+', newM: '+str(newM))

    # New p,q,m values
```

```
    pp = int(X/abs(m))
    qq = int(Y/abs(m))
    mm = int(newM/(m**2))
    print('pp: '+str(pp)+', qq: '+str(qq)+', mm: '+str(mm))

    # Determine if need to repeat
    if abs(mm)==1:
        if repeat==True:
            return (pp,qq,mm,counter,repeat)
        else:
            repeat = True
            return(findCyc(pp,qq,mm,N,counter,repeat))
    else:
        return(findCyc(pp,qq,mm,N,counter,repeat))

# Solving equation m*alpha - q*beta = p
def findSoln(m,q,p):
    # Rearrange: Solve for p + q*beta = m*alpha
    # Want p + q*beta divisible by m
    for beta in range(1,2*N):
        if (p+q*beta)%m==0:
            alpha = int((p+q*beta)/m)
            return(alpha,beta)
    else:
        return(0,0)

print("Please input an integer N that is not a square such that"\
      " x^2 - Ny^2 = 1 is the equation to be solved.")
print()
print("N: ")
in_N = input()
N = int(in_N)
print()

# Check if N is a square
if math.sqrt(N).is_integer():
    print('Please input an integer N such that N is not a square.')

else:
    print("Your equation input: x^2 - "+str(N)+"y^2 = 1")
    print()

    # Find first solution
    p,q,m = firstEq(N)
    print('p: '+str(p)+', q: '+str(q)+', m: '+str(m))

    # If gcd(q,m) != 1, compute gcd[(q,m),p] = d
    #   Then take (p/d, q/d, m/d^2)
```

```
div = findGCD(q,m)
#print(div)
if div != 1:
    d = findGCD(div,p)
    p = int(p/d)
    q = int(q/d)
    m = int(m/(d**2))

periodlength = findCyc(p,q,m,N,counter,repeat)
print()
#print(periodlength)
print('The length of the period is: '+str(periodlength[-2]))
```

References

[1] Datta, B., and Singh, A.N. *History of Hindu Mathematics: a source book, vol. 2*, Asia Publishing House, 1962.

[2] Dou, Ze-Li. Lecture notes on history of mathematics, Spring 2022.

[3] Dou, Ze-Li. Private communications.

[4] Heath, Thomas. *A History of Greek Mathematics, vol. II, from Aristarchus to Diophantus*, Clarendon Press, 1921.

[5] Katz, Victor J., Ed. *The Mathematics of Egypt, Mesopotamia, China, India, and Islam: a source book*, Princeton University Press, 2007.

[6] Lang, Serge. *Algebraic Number Theory*, Springer Verlag, 1986.

[7] Plofker, Kim. *Mathematics in India*, Princeton University Press, 2009.

[8] Rosen, Kenneth H. *Elementary Number Theory and Its Applications, Sixth Edition*, Addison-Wesley 2011.

[9] Shanks, Daniel. Solved and Unsolved Problems in Number Theory, Chelsea Publishing, 1962.

[10] Tate, John, and Silverman, Joseph. *Rational Points on Elliptic Curves*, Springer Verlag, 1992.

[11] Weil, André. *Number Theory: An approach through history from Hammurapi to Legendre*, Birhåuser, 1984.