5-8-2009

Applications of Continued Fractions in Cryptography and Diophantine Equations

Aaron H. Kaufer

Applications of Continued Fractions in Cryptography and Diophantine Equations

by

Aaron H. Kaufer

A thesis submitted in partial fulfillment of the
requirements for the degree of Master of Science
in the School of Mathematical Sciences
Rochester Institute of Technology

May 8, 2009

Committee:

Advisor	: Dr. Anurag Agarwal
Committee Member	: Prof. David S. Barth-Hart
Committee Member	: Dr. Manuel A. Lopez

Acknowledgements

I am greatly appreciative to several people who have made this thesis possible. First and foremost, I would like to thank my advisor Dr. Anurag Agarwal. Throughout the past three years, he has been an outstanding mentor. Since the first time I had him as a professor in number theory, he has taught me that the key to solving a problem is through persistent and rigorous thinking. I am grateful for his unwavering patience when teaching me new concepts, which has given me a new sense of confidence in my mathematical skills.

I would also like to thank the other two committee members, Professor David Barth-Hart and Dr. Manuel Lopez for expressing interest in my research and sharing their own ideas with me. They, too, have taught me the value of persistence and rigor in thought and to always search for the underlying beauty of a problem.

My parents have also been very supportive of my interest in mathematics. They were initially pleased to hear that I planned to study mathematics and were determined to send me to a school where I would receive a solid education.

A very special thanks goes out to a lifelong family friend, Christine Neuwirth, for sparking my interest in mathematics and higher learning. I had little direction in high school, and Chris was determined to convince me of the importance of receiving a higher education. She taught me to take my studies seriously and how to think more soundly. Without her, I do not know where I would be today.

Abstract

The theory of continued fractions has applications in cryptographic problems and in solution methods for Diophantine equations. We will first examine the basic properties of continued fractions such as convergents and approximations to real numbers. Then we will discuss a computationally efficient attack on the RSA cryptosystem (Wiener's attack) based on continued fractions. Finally, using continued fractions and solutions of Pell's equation, we will show that the Diophantine equation

$$x^4 - kx^2y^2 + y^4 = 2^j \quad (j, k \in \mathbb{N})$$

has no nontrivial solutions for $j = 9, 10, 11$ given that $k > 2$ and k is not a perfect square.

Contents

Notation

$\mathbb{N} = \{1, 2, 3, \ldots\}$
$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$
$\mathbb{E} = \{2, 4, 6, \ldots\}$
$\mathbb{O} = \{1, 3, 5, \ldots\}$
$\mathbb{Q} =$ rational numbers
$\mathbb{I} =$ irrational numbers
$\mathbb{R} =$ real numbers

Chapter 1

Continued Fractions

1.1 Rational Numbers as Finite Continued Fractions

We say $q \in \mathbb{Q}$ has a ***finite continued fraction*** if q can be expressed as

$$q = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}} \tag{1.1}$$

The terms of the sequence $\{a_0, a_1, \ldots, a_n\}$ are called ***partial quotients*** with $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{N}$ for $i > 0$. A shorthand notation for finite continued fractions is $[a_0; a_1, a_2, \ldots, a_n]$.

We begin with a theorem that allows us to find the continued fraction of rational numbers.

Theorem 1.1. *Every rational number has a finite continued fraction and conversely every finite continued fraction is a rational number.*

Proof. To prove the first direction, let $q = r_0/r_1$ where $r_0 \in \mathbb{Z}$ and $r_1 \in \mathbb{N}$ such that

$gcd(r_0, r_1) = 1$. Consider the following equations that arise from the Euclidean algorithm

$$\begin{aligned} r_0 &= a_0 r_1 + r_2 \\ r_1 &= a_1 r_2 + r_3 \\ &\vdots \\ r_{n-1} &= a_{n-1} r_n + r_{n+1} \\ r_n &= a_n r_{n+1} \end{aligned}$$

Since r_0 and r_1 are relatively prime, we have $r_{n+1} = 1$ and $r_n = a_n$. We may rewrite each equation

$$r_i = a_i r_{i+1} + r_{i+2}$$

as

$$\frac{r_i}{r_{i+1}} = a_i + \frac{r_{i+2}}{r_{i+1}} \tag{1.2}$$

By (1.2) we have

$$q = \frac{r_0}{r_1} = a_0 + \frac{r_2}{r_1} = a_0 + \frac{1}{a_1 + \frac{r_3}{r_2}} = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2 + \frac{r_4}{r_3}}} \cdots$$

$$= a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1+\frac{r_{n+1}}{r_n}}}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \frac{1}{a_n}}}}$$

The second direction can be proved using the concept of convergents, which are discussed in the following section. □

1.2 Convergents of Finite Continued Fractions

Let $q \in \mathbb{Q}$ such that $q = [a_0; a_1, \ldots, a_n]$, then $[a_0; a_1, \ldots, a_i]$ with $0 \leq i \leq n$ is called the i^{th} ***convergent*** of q. In order to compute the convergents of q, it is convenient to define the two recurrence relations

$$\begin{aligned} h_i &= a_i h_{i-1} + h_{i-2} \\ k_i &= a_i k_{i-1} + k_{i-2} \end{aligned} \tag{1.3}$$

with $h_{-1} = 1$, $k_{-1} = 0$, $h_{-2} = 0$ and $k_{-2} = 1$. To see how these recurrence relations relate to computing convergents we calculate the first three convergents of q.

$$\begin{aligned} [a_0] &= \frac{a_0}{1} = \frac{a_0 h_{-1} + h_{-2}}{a_0 k_{-1} + k_{-2}} = \frac{h_0}{k_0} \\ [a_0; a_1] &= \frac{a_1 a_0 + 1}{a_1} = \frac{a_1 h_0 + h_{-1}}{a_1 k_0 + k_{-1}} = \frac{h_1}{k_1} \\ [a_0; a_1, a_2] &= \frac{a_2(a_1 a_0 + 1) + a_0}{a_2 a_1 + 1} = \frac{a_2 h_1 + h_0}{a_2 k_1 + k_0} = \frac{h_2}{k_2} \end{aligned}$$

Before we prove that h_i/k_i is the i^{th} convergent of q, we need the following lemma.

Lemma 1.2. *Given that $[a_0; a_1, \ldots, a_i]$ is the i^{th} convgerent of q, then $\left[a_0; a_1, \ldots, a_i + \frac{1}{a_{i+1}}\right]$ is the $(i+1)^{st}$ convergent of q.*

Proof. The lemma is proved by the following reasoning

$$\left[a_0; a_1, \ldots, a_i + \frac{1}{a_{i+1}}\right] = a_0 + \cfrac{1}{\ddots + \cfrac{1}{a_i + \cfrac{1}{a_{i+1}}}} = [a_0; a_1, \ldots, a_i, a_{i+1}]$$

and so $[a_0; a_1, \ldots, a_i, a_{i+1}]$ is the $(i+1)^{st}$ convergent of q. □

Theorem 1.3. *Suppose $q \in \mathbb{Q}$ has the continued fraction $[a_0; a_1, \ldots, a_n]$. Then h_i/k_i is the i^{th} convergent of q, where h_i and k_i are defined in (1.3).*

Proof. We assume that h_{i-1}/k_{i-1} is the $(i-1)^{st}$ convergent of q. By Lemma 1.2 we can express the i^{th} convergent of q in the following way

$$\begin{aligned}\left[a_0; a_1, \ldots, a_{i-1} + \frac{1}{a_i}\right] &= \frac{(a_{i-1} + \frac{1}{a_i})h_{i-2} + h_{i-3}}{(a_{i-1} + \frac{1}{a_i})k_{i-2} + k_{i-3}} \\ &= \frac{a_i(a_{i-1}h_{i-2} + h_{i-3}) + h_{i-2}}{a_i(a_{i-1}k_{i-2} + k_{i-3}) + k_{i-2}} \\ &= \frac{a_i h_{i-1} + h_{i-2}}{a_i k_{i-1} + k_{i-2}} = \frac{h_i}{k_i}\end{aligned}$$

□

Suppose $q = [a_0; a_1, \ldots, a_n]$. We define q_i as

$$q_i = [a_i; a_{i+1}, \ldots, a_n] \quad (0 \leq i \leq n) \tag{1.4}$$

This definition leads to the following lemma.

Lemma 1.4. *For every $q \in \mathbb{Q}$*

$$q = \frac{q_i h_{i-1} + h_{i-2}}{q_i k_{i-1} + k_{i-2}} \quad (0 \leq i \leq n) \tag{1.5}$$

Proof. The reader may refer to [6, pp. 329–330]. □

Since convergents play a fundamental role in approximations to real numbers, we now state some lemmas concerning the central properties of convergents.

Lemma 1.5. *The sequence $\{k_1, k_2, \ldots, k_n\}$ defined in (1.3) is strictly increasing.*

Proof. Since we have $k_1 = a_1 \geq 1$ and $k_2 = a_2 a_1 + 1$, it is clear that $k_2 > k_1$. Suppose $k_{i-1} > k_{i-2}$. Since

$$k_i = a_i k_{i-1} + k_{i-2}$$

it is clear that $k_i > k_{i-1}$. Hence, the sequence is strictly increasing. □

Lemma 1.6. *Let $C_i = h_i/k_i$ be the i^{th} convergent of $[a_0; a_1, \ldots a_n]$. Then*

$$h_i k_{i-1} - h_{i-1} k_i = (-1)^{i-1} \quad (i \geq 1) \tag{1.6}$$

Proof. The reader may refer to [2, pp. 314] or [6, pp. 330–331]. □

Corollary 1.7. *Given that $C_i = h_i/k_i$ is the i^{th} convergent of $[a_0; a_1, \ldots a_n]$, then for $i \geq 0$, $gcd(h_i, k_i) = 1$.*

Proof. Let $g = gcd(h_i, k_i)$. Then by Lemma 1.6 we have $g|(-1)^{i-1}$ which implies $g = 1$. □

Lemma 1.8. *The sequence of convergents $\{C_0, C_1, \ldots, C_n\}$ of $[a_0; a_1, \ldots a_n]$ are ordered as follows*

$$\begin{aligned} &C_0 < C_2 < \ldots < C_n < C_{n-1} < \ldots < C_3 < C_1 \qquad (n \in \mathbb{E}) \\ &C_0 < C_2 < \ldots < C_{n-1} < C_n < \ldots < C_3 < C_1 \qquad (n \in \mathbb{O}) \end{aligned} \tag{1.7}$$

Proof. The reader may refer to [2, pp. 317–318] or [6, pp. 331]. □

1.3 Infinite Continued Fractions and Approximations to Real Numbers

We now turn our attention to infinite continued fractions. We say $s \in \mathbb{I}$ has an ***infinite continued fraction*** if

$$s = \lim_{n \to \infty} [a_0; a_1, \ldots, a_n] \tag{1.8}$$

This definition allows us to carry the properties of convergents of finite continued fractions over to infinite continued fractions. With this in mind we state an essential theorem concerning infinite continued fractions.

Theorem 1.9. *Every irrational number has an infinite continued fraction and conversely every infinite continued fraction is an irrational number.*

Proof. The reader may refer to [2, pp. 323 and 326] or [6, pp. 335]. □

We now discuss how to use continued fractions to approximate real numbers. The next theorem is crucial to the theory of rational approximations to real numbers.

Theorem 1.10. *Let $C_i = h_i/k_i$ be the i^{th} convergent of $r \in \mathbb{R}$. Then for any $a, b \in \mathbb{Z}$*

$$\left| r - \frac{h_i}{k_i} \right| \leq \left| r - \frac{a}{b} \right| \quad (1 \leq b \leq k_i) \tag{1.9}$$

Proof. The reader may refer to either [2, pp. 331] or [6, pp. 338–339]. □

Theorem 1.10 suggests that C_i is the best rational approximation for its denominator to r.

The heart of the theory of rational approximations to real numbers is contained in the next theorem and plays a central role in solving diophantine equations and attacking the RSA cryptosystem.

Theorem 1.11. *Let $r \in \mathbb{R}$. For any $a, b \in \mathbb{Z}$ with $gcd(a, b) = 1$ such that*

$$\left| r - \frac{a}{b} \right| < \frac{1}{2b^2} \quad (b \geq 1) \tag{1.10}$$

then a/b is a convergent of r.

Proof. The reader may refer to either [2, pp. 332] or [6, pp. 339]. □

1.4 Periodic Continued Fractions and Numbers of the Form $\sqrt{(na)^2 + a}$

We say $s \in \mathbb{I}$ has a ***periodic continued fraction*** if

$$s = [a_0; a_1, \ldots, a_n, \overline{a_{n+1}, a_{n+2}, \ldots, a_{n+p}}] \tag{1.11}$$

where $\overline{a_{n+1}, a_{n+2}, \ldots, a_{n+p}}$ indicates that the sequence $\{a_{n+1}, a_{n+2}, \ldots, a_{n+p}\}$ is repeated indefinitely. Furthermore, we say p is the ***period*** of the continued fraction.

Theorem 1.12. *Every quadratic irrational number has a periodic continued fraction and conversely every periodic continued fraction is a quadratic irrational number.*

Proof. The reader may refer to [6, pp. 345–348]. □

One of the aspects of the proof to Theorem 1.12 provides an algorithm for determining the continued fraction expansion of a quadratic irrational number. This algorithm is vital for solving Pell equations because it allows us to efficiently find the continued fraction expansion of $\sqrt{d} \in \mathbb{I}$.

Algorithm 1.13. *Let r be a quadratic irrational number with $r = r_0$ and let*

$$r_i = \frac{m_i + \sqrt{d}}{q_i} \quad (\sqrt{d} \in \mathbb{I}, m_i, q_i \in \mathbb{Z}) \tag{1.12}$$

with $\sqrt{d} \in \mathbb{I}$ and $m_i, q_i \in \mathbb{Z}$. Let a_i be the ith partial quotient of r. Then

$$a_i = \lfloor r_i \rfloor \tag{1.13}$$

with the iterative scheme

$$m_{i+1} = a_i q_i - m_i \tag{1.14}$$

and

$$q_{i+1} = \frac{d - m_{i+1}^2}{q_i} \tag{1.15}$$

Lemma 1.14. *Given $\sqrt{d} \in \mathbb{I}$ then*

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \ldots, a_{p-1}, 2a_0}] \tag{1.16}$$

and from Algorithm 1.13 we have $q_i = 1$ iff $p|i$ and $q_i \neq -1$ for all i.

Proof. The reader may refer to [6, pp. 350]. □

We now consider numbers of the form

$$\sqrt{(na)^2 + a} \quad (a, n \in \mathbb{N}) \tag{1.17}$$

We note that $(na)^2 + a$ cannot be a square because if it were then

$$b^2 = (na)^2 + a \quad (b \in \mathbb{N})$$

This allows us to express a as

$$a = b^2 - (na)^2 = (b - na)(b + na)$$

Thus $(b + na)|a$ which is a contradiction. Since $\sqrt{(na)^2 + a}$ is irrational, we can use Algorithm 1.13 to find its continued fraction. The following table gives the values of m_i, q_i and a_i.

i	m_i	q_i	a_i
0	0	1	na
1	na	a	$2n$
2	na	1	$2na$
3	na	a	$2n$

We see from the table that $p = 2$ given that $a \neq 1$ because row 1 and row 3 are identical. Hence

$$\sqrt{(na)^2 + a} = [na; \overline{2n, 2na}] \tag{1.18}$$

Observe that if $a = 1$ then $p = 1$; however we still refer to (1.18) for the continued fraction of $\sqrt{(na)^2 + a}$.

Chapter 2

Continued Fractions and the RSA Cryptosystem

2.1 The RSA Cryptosystem

The RSA Cryptosytem is a public key cryptosystem invented by Ron Rivest, Adi Shamir and Leonard Adleman. Consider the following scenario: suppose Alice wants to send a message to Bob over an insecure channel. Let us further suppose that Alice does not want an eavesdropper named Eve to be able to read her message over the channel. How can Alice securely send her message to Bob? We investigate how the RSA cryptosystem provides a possible solution to this problem.

To see how the RSA cryptosystem works, let us assume that Bob is expecting to receive a message from Alice. Alice cannot simply send the message to Bob because Eve can easily read the message if she were to intercept it. Therefore Alice must first encode her message in such a way that Bob can easily decode the message and Eve cannot. Let us assume that Alice and Bob decide to encode/decode the message using the RSA cryptosystem. First Bob chooses a large integer N such that $N = pq$ where p and q are distinct large primes.

Since Bob knows p and q he can compute

$$\phi(N) = (p-1)(q-1) \tag{2.1}$$

He next chooses two numbers e and d with $1 < e, d < \phi(N)$ such that

$$ed \equiv 1 \pmod{\phi(N)} \tag{2.2}$$

Bob's *private key* is (p, q, d) and his *public key* is (N, e). Since Bob is expecting a message from Alice, he sends his public key across the channel to her (he does not care if Eve intercepts it). Upon receiving Bob's public key, Alice encodes her message m (we assume that $m < N$, if it is not then Alice can send her message in blocks) using the encryption function

$$E(m) \equiv m^e \pmod{N}$$

She then sends m^e to Bob across the same channel. Bob is now able to decode m^e using the decryption function

$$D(m^e) \equiv (m^e)^d \equiv m^{ed} \pmod{N}$$

We claim that $m^{ed} \equiv m \pmod{N}$ and hence Bob has recovered Alice's message. For a more in depth discussion of the RSA cryptosystem, the reader may refer to [5, Chapter 3].

2.2 Wiener's Attack on the RSA Cryptosystem

We now discuss an attack on the RSA cryptosystem that utilizes continued fractions, which was published by Wiener. The reader may refer to Wiener's original article [7] for more information. We cite the more recent article [4] as the primary source for our discussion of Wiener's attack.

In order to remove some ambiguity from the analysis we let $N = pq$ where p and q are odd primes and determine the smallest $a \in \mathbb{N}$ such that $p < q < ap$. Since $ed \equiv 1$

$(\mathrm{mod}\ \phi(N))$, we may rewrite this expression as

$$\phi(N) = \frac{ed-1}{k} \quad (k \in \mathbb{N}) \tag{2.3}$$

The main idea of Wiener's attack is to show that certain restrictions of d allow for the fraction k/d to be a convergent of e/N. We begin our discussion of Wiener's attack with the following lemma.

Lemma 2.1. *Let $N = pq$ where p and q are distinct primes such that $p < q < ap$ for some $a \in \mathbb{N}$. Then*

$$N - (a+1)\sqrt{N} < \phi(N) < N \tag{2.4}$$

Proof. We first prove $\phi(N) < N$. Clearly

$$(p-1)(q-1) < pq$$

We next prove $N - (a+1)\sqrt{N} < \phi(N)$. We begin with

$$\sqrt{N} > p > p - \frac{1}{a+1}$$

This statement implies

$$\begin{aligned}(a+1)\sqrt{N} &> (a+1)p - 1 \\ &> (p+q) - 1\end{aligned}$$

Finally

$$N - (a+1)\sqrt{N} < N - (p+q) + 1 = \phi(N)$$

□

With this fact now established, we investigate the conditions for which k/d will be a convergent of e/N. We consider another lemma.

Lemma 2.2. *Let (N, e) be the public key with $N = pq$ such that $p < q < ap$ for some $a \in \mathbb{N}$. Furthermore let k and d be defined from (2.3). Then*

$$\left| \frac{e}{N} - \frac{k}{d} \right| < \frac{(a+1)k}{d\sqrt{N}} \tag{2.5}$$

Proof. By Lemma 2.1 and (2.3) we have

$$k(N - (a+1)\sqrt{N}) < ed - 1$$

Dividing the inequality by dN and rearranging yields

$$\frac{k}{d} - \frac{e}{N} < \frac{(a+1)k}{d\sqrt{N}} - \frac{1}{dN} \tag{2.6}$$

Furthermore, we see that

$$ed + 1 = k\phi(N) + 2 < kN + (a+1)k\sqrt{N}.$$

Rearranging and dividing the inequality by dN yields

$$-\left(\frac{(a+1)k}{d\sqrt{N}} - \frac{1}{dN} \right) < \frac{k}{d} - \frac{e}{N} \tag{2.7}$$

Combining (2.6) and (2.7) gives

$$\begin{aligned} \left| \frac{e}{N} - \frac{k}{d} \right| &< \frac{(a+1)k}{d\sqrt{N}} - \frac{1}{dN} \\ &< \frac{(a+1)k}{d\sqrt{N}} \end{aligned}$$

□

We are almost in a position to examine the required conditions on d that allow for k/d to be a convergent of e/N. However, we first prove another lemma.

Lemma 2.3. *Let k and d be defined from (2.3). Then $k < d$.*

Proof. Rearranging (2.3) and using the fact that $e < \phi(N)$ yields

$$\frac{d}{k} = \frac{k\phi(N) + 1}{ek} > 1$$

Hence $k < d$. □

We are now ready to prove Wiener's main result that k/d is a convergent of e/N for certain values of d. In order to do this, we appeal to Theorem 1.11 by examining when

$$\left| \frac{e}{N} - \frac{k}{d} \right| < \frac{1}{2d^2} \tag{2.8}$$

Theorem 2.4. *We have k/d as a convergent of e/N provided that*

$$d \leq \frac{\sqrt[4]{N}}{\sqrt{2(a+1)}} \tag{2.9}$$

Proof. By Theorem 1.11 and Lemma 2.2, k/d is a convergent of e/N if

$$\frac{(a+1)k}{d\sqrt{N}} < \frac{1}{2d^2} \tag{2.10}$$

We proceed with the fact that (2.10) is true iff $2(a+1)kd < \sqrt{N}$. Lemma 2.3 implies

$$2(a+1)kd < 2(a+1)d^2$$

We maximize d by letting $2(a+1)d^2 \leq \sqrt{N}$ which yields

$$d \leq \frac{\sqrt[4]{N}}{\sqrt{2(a+1)}}$$

□

Observe from the previous theorem that the bound of d depends on a. As the value of a increases, the value of d that guarantees k/d to be a convergent of e/N decreases.

We determine which convergent is k/d by a clever way of factoring N. Suppose we are able to express N as

$$N = x^2 - y^2 = (x - y)(x + y) \quad (x, y \in \mathbb{N}) \tag{2.11}$$

Since $N = pq$, we have either $p = x - y$ and $q = x + y$ or $1 = x - y$ and $N = x + y$. Solving for x and y in the first and second cases respectively gives

$$\begin{aligned} x &= \frac{q + p}{2} & y &= \frac{q - p}{2} \\ x &= \frac{N + 1}{2} & y &= \frac{N - 1}{2} \end{aligned} \tag{2.12}$$

This method of factoring N is called *Fermat's Factorization Algorithm*; for more information see [3, pp. 37–40].

We now see how to use these observations in Wiener's attack to determine the private key (p, q, d). Assuming $N = x^2 - y^2$ and (2.9) is satisfied, we test each convergent sequentially. Let k'/d' be the convergent of e/N that we are testing. For each convergent k'/d', let $\phi'(N)$, x' and y' be defined as follows

$$\phi'(N) = \frac{ed' - 1}{k'} \tag{2.13}$$

$$x' = \frac{N - \phi'(N) + 1}{2} \tag{2.14}$$

$$y' = \sqrt{(x')^2 - N} \tag{2.15}$$

The following theorem is known as the *Wiener Test* which tells us how to use x' and y' to find (p, q, d).

Theorem 2.5 (Wiener Test). *Let k'/d' be a convergent of e/N. If $x', y' \in \mathbb{N}$ where x' and y' are defined in (2.14) and (2.15) then the private key*

$$(p, q, d) = (x' - y', x' + y', d') \tag{2.16}$$

Proof. Since $x', y' \in \mathbb{N}$, by (2.15) we have

$$N = (x')^2 - (y')^2 = (x' - y')(x' + y')$$

Suppose $x' = (N + 1)/2$, then (2.13) and (2.14) give

$$N + 1 = N - \frac{ed' - 1}{k'} + 1$$

which is only satisfied if $e = 1$. However, since $e > 1$, by (2.12) we have

$$x' = \frac{q + p}{2} \qquad\qquad y' = \frac{q - p}{2}$$

Using (2.14) we have

$$\phi'(N) = N - (p + q) + 1 = \phi(N)$$

Since $\phi'(N) = \phi(N)$ it follows that

$$d' \equiv d \pmod{\phi(N)}$$

However, Lemma 1.5 guarantees $d' \not> d$ because we are testing the convergents sequentially and since $1 < d < \phi(N)$, it follows that $d' = d$. □

Example 2.6. *Let $N = 826513$ and $e = 589063$. Use Wiener's attack to show that $(p, q, d) = (829, 997, 7)$.*

Proof. We begin with

$$\frac{e}{N} = [0; 1, 2, 2, 12, 1, 1, 19, 1, 2, 5, 2, 6]$$

The first three convergents are $0/1$, $1/1$ and $2/3$ and all fail the Wiener test. We apply Wiener's test to the next convergent $5/7$. We begin with

$$\phi'(N) = \frac{7e-1}{5} = 824688$$

which gives $x' = 913$ and $y' = 84$. Since $x, y \in \mathbb{N}$, by Theorem 2.5, $5/7$ is the correct convergent and so (p, q, d) = $(829, 997, 7)$. □

The next example is designed to illustrate an important point. The largest bound on d occurs when $a = 2$ which gives

$$d \leq \frac{\sqrt[4]{N}}{\sqrt{6}} \tag{2.17}$$

However this condition is only sufficient but not necessary for the Wiener attack to succeed.

Example 2.7. *Let* $N = 826513$ *and* $e = 697813$. *Use Wiener's attack to show that* $(p, q, d) = (829, 997, 13)$.

Proof. We note that by (2.17) the largest bound on d is 12. Now

$$\frac{e}{N} = [0; 1, 5, 2, 2, 1, 2, 2, 1, 1, 13, 1, 1, 1, 3, 3, 2]$$

The convergents with $d \leq 12$ are $0/1$, $1/1$ and $5/6$. However, all three convergents fail the Wiener test. The next convergent is $11/13$. Since $13 > 12$, the attack is no longer guaranteed to work. However, the Wiener test yields

$$\phi'(N) = \frac{13e-1}{11} = 824688$$

Since we have used the same N as in the previous example and $\phi'(N)$ is identical to $\phi(N)$ in the previous example, we have chosen the correct convergent. Thus (p, q, d) = $(829, 997, 13)$. □

Chapter 3

Pell's Equation

3.1 The Pell Equation

The primary focus of this chapter is to use continued fractions to solve Pell Equations. The ***Pell Equation*** is defined as

$$x^2 - dy^2 = N \quad (N \in \mathbb{Z}) \tag{3.1}$$

Note that (3.1) has only a finite number of solutions if $d \leq 0$ or d is a perfect square. Therefore we assume that $d > 0$ and is not a perfect square. We say (X, Y) is a ***nontrivial solution*** of (3.1) if both $X \neq 0$ and $Y \neq 0$. Observe that if (X, Y) is a solution of (3.1) then $(\pm X, \pm Y)$ are also solutions of (3.1). Thus we may restrict X and Y so that $X, Y > 0$. Furthermore, we say (X, Y) is a ***primitive solution*** of (3.1) if (X, Y) is a nontrivial solution such that $gcd(X, Y) = 1$.

3.2 Case: $x^2 - dy^2 = 1$

Consider the Pell equation

$$x^2 - dy^2 = 1 \tag{3.2}$$

The following theorem provides us with infinitely many primitive solutions of (3.2).

Theorem 3.1. *Let h_{ip-1}/k_{ip-1} be a convergent of $\sqrt{d} \in \mathbb{I}$ where p is the period of the continued fraction of $\sqrt{d}$. Then*

$$h_{ip-1}^2 - dk_{ip-1}^2 = (-1)^{ip} \quad (i \geq 1) \tag{3.3}$$

Proof. By Algorithm 1.13 and Lemma 1.4 we can write

$$\sqrt{d} = \frac{(m_{n+1} + \sqrt{d})h_n + q_{n+1}h_{n-1}}{(m_{n+1} + \sqrt{d})k_n + q_{n+1}k_{n-1}}$$

Rearranging this equation yields

$$(m_{n+1}k_n + q_{n+1}k_{n-1} - h_n)\sqrt{d} = m_{n+1}h_n + q_{n+1}h_{n-1} - dk_n$$

Since the right-hand side of the equation is rational, the only way for the left-hand side of the equation to be rational is if both sides of the equation are equal to zero. We now solve for m_{n+1} which leads to

$$m_{n+1} = \frac{h_n - q_{n+1}k_{n-1}}{k_n} = \frac{dk_n - q_{n+1}h_{n-1}}{h_n}$$

By Lemma 1.6

$$h_n^2 - dk_n^2 = q_{n+1}(h_nk_{n-1} - h_{n-1}k_n) = q_{n+1}(-1)^{n+1}$$

By Lemma 1.14, if $n = ip - 1$ then

$$h_{ip-1}^2 - dk_{ip-1}^2 = q_{ip}(-1)^{ip} = (-1)^{ip}$$

□

Corollary 3.2. *If $p \in \mathbb{E}$ then h_{ip-1}/k_{ip-1} is a solution of (3.2) for all $i \in \mathbb{N}$, otherwise h_{ip-1}/k_{ip-1} is a solution of (3.2) for all $i \in \mathbb{E}$.*

Proof. This can be easily verified by checking (3.3) for each case. □

We now discuss fundamental solutions. We say (X_1, Y_1) is the ***fundamental solution*** of (3.2) if X_1/Y_1 is the first convergent of $\sqrt{d}$ that is a nontrivial solution of (3.2). By Corollary 3.2, the fundamental solution of (3.2) is

$$\begin{aligned} &(h_{p-1}, k_{p-1}) \quad (p \in \mathbb{E}) \\ &(h_{2p-1}, k_{2p-1}) \quad (p \in \mathbb{O}) \end{aligned} \tag{3.4}$$

The concept of a fundamental solution is important because it allows us to generate every solution of (3.2) by a recursive sequence.

Theorem 3.3. *Let (X_1, Y_1) be the fundamental solution of (3.2). Then every positive solution of (3.2) denoted by (X_n, Y_n) where $n \in \mathbb{N}$ is given by the coefficients of $(X_1 + Y_1\sqrt{d})^n$. Hence X_n and Y_n can be found by the following recurrence relations*

$$\begin{aligned} X_n &= X_1X_{n-1} + dY_1Y_{n-1} \\ Y_n &= X_1Y_{n-1} + X_{n-1}Y_1 \end{aligned} \tag{3.5}$$

Proof. The reader may refer to [6, pp. 354–355]. □

3.3 Case $N > 1$: $x^2 - dy^2 = N$

We now consider methods for finding infinitely many solutions of the Pell equation

$$x^2 - dy^2 = N \quad (N > 1) \tag{3.6}$$

Lemma 3.4. *If (W,Z) is a solution of (3.6) and (X, Y) is a solution to (3.2) then*

$$(WX + dYZ, XZ + WY) \tag{3.7}$$

is also a solution of (3.6).

Proof. Suppose that (W,Z) is a solution of (3.6) and (X, Y) is a solution of (3.2). Then

$$\begin{aligned} N &= (X^2 - dY^2)(W^2 - dZ^2) \\ &= (WX)^2 + (dYZ)^2 - d[(XZ)^2 + (WY)^2] \\ &= (WX)^2 + 2dWXYZ + (dYZ)^2 - d[(XZ)^2 + 2WXYZ + (WY)^2] \\ &= (WX + dYZ)^2 - d(XZ + WY)^2 \end{aligned}$$

Therefore $(WX + dYZ, XZ + WY)$ is also a solution of (3.6). □

Suppose we have calculated the fundamental solution of (3.2). Since Theorem 3.3 provides us with infinitely many solutions of (3.2) and multiplying each solution by $W^2 - dZ^2$ produces a new solution of (3.6), Theorem 3.3 and Lemma 3.4 allow us to find infinitely many solutions of (3.6). Furthermore, we say that two solutions (A, B) and (C, D) of (3.6) are in different ***solution classes*** if there does not exist a solution (X, Y) of (3.2) such that either $(A, B) = (CX + dDY, DX + CY)$ or $(C, D) = (AX + dBY, BX + AY)$. Additionally, we say (W_1, Z_1) is the ***fundamental solution of its class*** if W_1 and Z_1 are respectively the least positive and least nonnegative integers of their class that satisfy (3.6). Likewise, we say (W, Z) is the ***minimal positive solution of its class*** if both W and Z are the least positive integers of their class that satisfy (3.6). Let C be a solution class of (3.6). Then every $(W_n, Z_n) \in C$ is generated as follows

$$W_n + Z_n\sqrt{d} = (W_1 + Z_1\sqrt{d})(X_1 + Y_1\sqrt{d})^n \quad (n \in \mathbb{N}) \tag{3.8}$$

Theorem 3.5. *Let (X_1, Y_1) be the fundamental solution of (3.2) and (W_1, Z_1) be the fundamental solution of its class of (3.6) then*

$$\begin{aligned} 0 < W_1 &\leq \sqrt{\frac{N(X_1 + 1)}{2}} \\ 0 \leq Z_1 &\leq \frac{Y_1\sqrt{N}}{\sqrt{2(X_1 + 1)}} \end{aligned} \tag{3.9}$$

Proof. The reader may refer to [1, pp. 26–28]. □

Lemma 3.6. *There are only finitely many solution classes of (3.1).*

Proof. See [1, pp. 24] for details and references. □

Theorem 3.7. *Suppose (3.6) has t solutions classes with $(W_{1,i}, Z_{1,i})$ as the fundamental solution for each class where $1 \leq i \leq t$. Let (X_1, Y_1) be the fundamental solution of (3.2) and let the set S be defined as*

$$S = \bigcup_{i=1}^{t} \{(W_{1,i} + Z_{1,i}\sqrt{d})(X_1 + Y_1\sqrt{d})^n\} \quad (n \in \mathbb{N}) \tag{3.10}$$

Then S contains every positive solution of (3.6).

Proof. See [1, pp. 28] for details and references. □

3.4 Case $0 < N < \sqrt{d}$: $x^2 - dy^2 = N$

Consider the Pell equation

$$x^2 - dy^2 = N \quad (N < \sqrt{d}) \tag{3.11}$$

The following theorem establishes the connection between the convergents of $\sqrt{d}$ and the solutions of (3.11).

Theorem 3.8. *If (X, Y) is a solution of (3.11) then X/Y is a convergent of $\sqrt{d}$.*

Proof. Since (X, Y) is a solution of (3.11) we may write

$$N = X^2 - dY^2 = (X - Y\sqrt{d})(X + Y\sqrt{d})$$

Since $\sqrt{d} > N > 0$, we have

$$0 < \frac{X}{Y} - \sqrt{d} < \frac{N}{Y(X + Y\sqrt{d})} < \frac{\sqrt{d}}{Y(X + Y\sqrt{d})}$$

Since $Y\sqrt{d} < X$, we have $2Y\sqrt{d} < X + Y\sqrt{d}$ and so

$$0 < \frac{X}{Y} - \sqrt{d} < \frac{\sqrt{d}}{Y(X + Y\sqrt{d})} < \frac{1}{2Y^2}$$

Thus we have

$$\left|\frac{X}{Y} - \sqrt{d}\right| < \frac{1}{2Y^2} \tag{3.12}$$

By (3.12), it follows that X/Y is a convergent of $\sqrt{d}$ by Theorem 1.11. □

Corollary 3.9. *If (X, Y) is a primitive solution of (3.11) then there is some convergent h_i/k_i of $\sqrt{d}$ as defined in (1.3) such that $X = h_i$ and $Y = k_i$.*

Proof. Since (X, Y) is a primitive solution, we have $gcd(X, Y) = 1$ and from Lemma 1.7 we also have $gcd(h_i, k_i) = 1$. The result now follows immediately from Theorem 3.8. □

Now that we have established Corollary 3.9, we discuss solution methods of (3.11). By letting $g = gcd(X, Y)$ we may write $X = gU$ and $Y = gV$. Substituting these values into (3.11) gives

$$U^2 - dV^2 = \frac{N}{g^2}$$

Hence (U, V) is a primitive solution of the Pell equation

$$x^2 - dy^2 = \frac{N}{g^2} \tag{3.13}$$

Now that we have an acquaintance with the notion of solution classes, we give the following algorithm for finding every minimal positive solution of (3.11). This algorithm is a consequence of Theorem 3.8.

Algorithm 3.10. *In order to find the minimal positive solutions of (3.11), we first find the fundamental solution of (3.2) which we call (h_m, k_m), where h_m/k_m is the m^{th} convergent of $\sqrt{d}$. For each i with $0 \leq i \leq m$ such that*

$$h_i^2 - dk_i^2 = \frac{N}{g^2} \quad \left(\frac{N}{g^2} \in \mathbb{N}\right) \tag{3.14}$$

we have (gh_i, gk_i) *as a minimal positive solution of (3.11). Let* H *be the set of all solutions* (gh_i, gk_i) *with* $0 \leq i \leq m$ *such that* (h_i, k_i) *satisfies (3.14). Then* H *contains every minimal positive solution of (3.11).*

Proof. For a discussion of the algorithm see [1, pp. 29–31]. □

3.5 Case: $x^2 - ((na)^2 + a)y^2 = 1$

Consider the Pell equation

$$x^2 - ((na)^2 + a)y^2 = 1. \tag{3.15}$$

By (1.18) and (3.4) we can conclude that $(X_1, Y_1) = (2n^2a + 1, 2n)$ is the fundamental solution of (3.15). By Theorem 3.3 we can find the family of solutions as

$$\begin{aligned} X_n &= (2n^2a + 1)X_{n-1} + 2n((na)^2 + a)Y_{n-1} \\ Y_n &= (2n^2a + 1)Y_{n-1} + 2nX_{n-1} \end{aligned} \tag{3.16}$$

By (3.16) we can express Y_n as

$$\begin{aligned} Y_1 &= 2n \\ Y_2 &= 4n(2n^2a + 1) \\ Y_n &= 2(2n^2a + 1)Y_{n-1} - Y_{n-2} \end{aligned} \tag{3.17}$$

Lemma 3.11. *If* (X, Y) *is a solution of (3.15) then* $Y \in \mathbb{E}$.

Proof. We have $Y_1, Y_2 \in \mathbb{E}$. If we assume $Y_{n-1}, Y_{n-2} \in \mathbb{E}$ then by (3.17) it follows that $Y_n \in \mathbb{E}$. □

Chapter 4

Thue-Mahler Quartic Equations

The focus of this chapter is to investigate the solutions of the quartic diophantine equation

$$x^4 - kx^2y^2 + y^4 = 2^j \quad (j, k \in \mathbb{N}) \tag{4.1}$$

We are interested in ***nontrivial solutions*** of (4.1) (where nontrivial solution is defined the same way as in Chapter 3). It has been shown in [1] that (4.1) has no nontrivial solutions when $1 \leq j \leq 8$ with $k > 2$ and k is not a square. The cases where $k = 2$ and k is a square have been completely settled in [1, pp. 48–51] as well. Therefore, this chapter focuses on showing that (4.1) has no nontrivial solutions when $j = 9, 10, 11$ with the following restrictions: $k \neq 2$ and k is not a square.

4.1 A Solution Method

We turn our attention to a method developed in [1] that is designed to show that (4.1) has no nontrivial solutions. The key idea is to look at (4.1) as a quadratic equation in x^2 which gives

$$x^2 = \frac{ky^2 \pm \sqrt{(k^2 - 4)y^4 + 2^{j+2}}}{2} \tag{4.2}$$

From (4.2) we see that the only way for x^2 to be an integer is if

$$u^2 = (k^2 - 4)y^4 + 2^{j+2} \quad (u \in \mathbb{N}) \tag{4.3}$$

If we let $v = y^2$ and rearrange the terms, (4.3) becomes

$$u^2 - (k^2 - 4)v^2 = 2^{j+2} \tag{4.4}$$

which is a Pell equation. If we are able to show that (4.4) has no solutions that satisfy (4.1) then we have shown that (4.1) has no nontrivial solutions for the specific j.

Let (X, Y) be a solution of (4.1). The following lemma reduces the possible values of X and Y that we need to check to show that (4.1) has no nontrivial solutions.

Lemma 4.1. *If there are no nontrivial solutions (X, Y) of (4.1) where X and Y have the same parity and $X > Y > 0$, then there are no nontrivial solutions of (4.1) for all $X, Y \in \mathbb{Z}$.*

Proof. Suppose (X,X) is a solution. Then (4.1) becomes

$$X^4(2 - k) = 2^j$$

but this equation has no solution since we are assuming that $k > 2$. It can be easily seen that $X \in \mathbb{E}$ iff $Y \in \mathbb{E}$, therefore X and Y must have the same parity. It is also evident that if (X, Y) is a solution then (Y, X) and $(\pm X, \pm Y)$ are solutions as well. Therefore, we only consider solutions such that $X > Y > 0$. □

We now discuss the ***primitive solutions*** of (4.1) (where primitive solution is defined the same way as in Chapter 3).

Lemma 4.2. *If (X, Y) is a solution of (4.1), then either $gcd(X, Y) = 1$ or $gcd(X, Y) = 2^m$ for some $m \in \mathbb{N}$.*

Proof. Let $g = gcd(X, Y)$. Then from (4.1) we have $g^4 | 2^j$. Consequently, either $g = 1$ or g is a nontrivial power of 2. □

The following two sections illustrate this method for $1 \leq j \leq 8$. The first of these sections outlines the method when $j \in \mathbb{E}$ and the second section outlines the method when $j \in \mathbb{O}$.

4.2 Case $j = 2$: $x^4 - kx^2y^2 + y^4 = 4$

We consider the quartic equation

$$x^4 - kx^2y^2 + y^4 = 4 \quad (k \in \mathbb{N}) \tag{4.5}$$

Theorem 4.3 (Agarwal). *Equation (4.5) has no nontrivial solutions when $k > 2$ and k is not a square.*

Proof. Suppose (X, Y) is a solution of (4.5) with $X, Y \in \mathbb{E}$. Let $X = 2U$ and $Y = 2V$. Then (4.5) becomes

$$16[U^4 - kU^2V^2 + V^4] = 4$$

which implies that $16|4$. This is a contradiction and so any solution to (4.5) must be primitive. Since $X, Y \in \mathbb{O}$ for any primtive solution (X, Y) to (4.5), it follows that $k \equiv 2 \pmod 4$ and so $k = 4s + 2$. Substituting k and j into (4.4) gives the following Pell equation

$$u^2 - (16s^2 + 16s)v^2 = 16 \tag{4.6}$$

From (4.6) we see that $16|u^2$ and so $4|u$. Letting $u = 4w$ and simplifying (4.6) gives

$$w^2 - (s^2 + s)v^2 = 1 \tag{4.7}$$

Let (S, T) be a solution of (4.7). Since (4.7) is of the form (3.15) with $n = 1$ and $a = s$, it follows by Lemma 3.11 that $T \in \mathbb{E}$. However this a contradiction since we have assumed that $Y \in \mathbb{O}$ and $T = Y^2$ implies that $Y \in E$. Therefore by Lemma 4.1 it follows that there are no nontrivial solutions of (4.5). □

The cases where $j = 4, 6, 8$ are proved in a similar manner in [1, pp. 51–64].

4.3 Case $j = 3$: $x^4 - kx^2y^2 + y^4 = 8$

We consider the quartic equation

$$x^4 - kx^2y^2 + y^4 = 8 \quad (k \in \mathbb{N}) \tag{4.8}$$

Theorem 4.4 (Agarwal). *Equation (4.8) has no nontrivial solutions when $k > 2$ and k is not a square.*

Proof. Suppose (X, Y) is a solution of (4.8) with $X, Y \in \mathbb{E}$. Let $X = 2U$ and $Y = 2V$. Then (4.8) becomes

$$16[U^4 - kU^2V^2 + V^4] = 8$$

which implies that $16|8$. This is a contradiction and so any solution to (4.8) must be primitive. Since $X, Y \in \mathbb{O}$ for any primtive solution (X, Y) to (4.8), we have $k \equiv 2 \pmod 8$ and so $k = 8s + 2$. Substituting k and j into (4.4) gives the following Pell equation

$$u^2 - (64s^2 + 32s)v^2 = 32 \tag{4.9}$$

From (4.9) we see that $32|u^2$ and so $8|u$. Letting $u = 8w$ and simplifying (4.9) gives

$$(2w)^2 - ((2s)^2 + 2s)v^2 = 2$$

Letting $b = 2w$, the previous equation becomes

$$b^2 - ((2s)^2 + 2s)v^2 = 2 \tag{4.10}$$

The fundamental solution of

$$b^2 - ((2s)^2 + 2s)v^2 = 1 \tag{4.11}$$

is $(4s+1, 2)$, and so by Theorem 3.5 it follows that for any fundamental solution (W_1, Z_1) of (4.10)

$$0 \leq Z_1 \leq \frac{\sqrt{2}}{\sqrt{2s+1}}$$

But since $s \geq 1$, we have $Z_1 \leq 0$ and so $Z_1 = 0$. Hence $b^2 = 2$, which is a contradiction and so there is no fundamental solution of (4.10) and thus no solution of (4.10) exists. Therefore by Lemma 4.1 it follows that there are no nontrivial solutions of (4.8). □

The cases where $j = 1, 5, 7$ are proved in a similar manner in [1, pp. 66–74].

4.4 Preliminaries for Cases $j \geq 9$

We now state some lemmas that help us prove (4.1) has no nontrivial when $j = 9, 10, 11$.

Theorem 4.5. *If a is an odd integer then $x^2 \equiv a \pmod{2^n}$ for $n \geq 3$ has a solution iff $a \equiv 1 \pmod{8}$.*

Proof. The reader may refer to [2, pp. 194–195]. □

Corollary 4.6. *Let (X, Y) be a solution of (4.1) with $X, Y \in \mathbb{O}$ and $j \geq 6$ then*

$$k \equiv 2 \pmod{64} \tag{4.12}$$

Proof. Since $j \geq 6$

$$X^4 - kX^2Y^2 + Y^4 \equiv 0 \pmod{64} \tag{4.13}$$

Since $X, Y \in \mathbb{O}$ then by Theorem 4.5

$$\begin{aligned} X^2 &\equiv 8a + 1 \pmod{64} \\ Y^2 &\equiv 8b + 1 \pmod{64} \end{aligned} \tag{4.14}$$

Substituting (4.14) into (4.13) and rearranging yields

$$k(8(a+b)+1) \equiv 2(8(a+b)+1) \pmod{64} \tag{4.15}$$

Since $gcd(64, 8(a+b)+1) = 1$, (4.15) reduces to

$$k \equiv 2 \pmod{64}$$

□

We now consider the following Pell equation

$$x^2 - ((na)^2 + a)v^2 = 2^r \quad (r \geq 2) \tag{4.16}$$

Lemma 4.7. *If 2^r is a square then $Z \in \mathbb{E}$ for every (W, Z) in the same solution class as $(2^{r/2}, 0)$.*

Proof. Observe that $(2^{r/2}, 0)$ is the fundamental solution of (4.16) for all a and let (X_1, Y_1) be the fundamental solution of

$$x^2 - ((na)^2 + a)v^2 = 1$$

Then by Lemma 3.4, $(2^{r/2}X_1, 2^{r/2}Y_1)$ is a solution of (4.16) and by (3.8), every solution (W, Z) in this class is of the form

$$\begin{aligned} W + Z\sqrt{d} &= (2^{r/2}X_1 + 2^{r/2}Y_1\sqrt{d})(X_1 + Y_1\sqrt{d})^i \quad (i \in \mathbb{N}) \\ &= 2^{r/2}(X_1 + Y_1\sqrt{d})^{i+1} \end{aligned}$$

which forces $Z \in \mathbb{E}$. □

Lemma 4.8. *Suppose $\sqrt{(na)^2 + a} > 2^r$. If 2^r is a square then every solution of (4.16) is in the same solution class as $(2^{r/2}, 0)$. If 2^r is not a square then (4.16) has no solutions.*

Proof. Since $\sqrt{(na)^2 + a} > 2^r$, we may apply Algorithm 3.10 to (4.16). The only possible solution occurs when $i = 1$ which gives some (X_1, Y_1) as the fundamental solution to

$$x^2 - ((na)^2 + a)v^2 = 1$$

If 2^r is not a square then (4.16) has no solutions. If 2^r is a square then Algorithm 3.10 produces $(2^{r/2}X_1, 2^{r/2}Y_1)$ as a solution of (4.16). Since $(2^{r/2}, 0)$ is the fundamental solution of (4.16), we have by (3.8) that $(2^{r/2}, 0)$ and $(2^{r/2}X_1, 2^{r/2}Y_1)$ are in the same class. □

4.5 Case $j = 9$: $x^4 - kx^2y^2 + y^4 = 2^9$

We consider the quartic equation

$$x^4 - kx^2y^2 + y^4 = 2^9 \quad (k \in \mathbb{N}) \tag{4.17}$$

Theorem 4.9. *Equation (4.17) has no nontrivial solutions when $k > 2$ and k is not a square.*

Proof. Suppose that (X, Y) is a solution of (4.17) with $X, Y \in \mathbb{E}$. Let $X = 2U$ and $Y = 2V$. Then (4.17) becomes

$$U^4 - kU^2V^2 + V^4 = 2^5$$

This would imply that (4.1) has a nontrivial solution when $j = 5$, which is is a contradiction. Therefore any solution of (4.17) must be primitive. Since $X, Y \in \mathbb{O}$ for any primtive solution (X, Y) of (4.17), by Corollary 4.6, $k \equiv 2 \pmod{64}$ and so $k = 64s + 2$. Substituting k and j into (4.4) gives the following Pell equation

$$u^2 - (2^{12}s^2 + 2^8 s)v^2 = 2^{11} \tag{4.18}$$

From (4.18) we see that $256|u^2$ and so $16|u$. Letting $u = 16w$ and simplifying (4.18) gives

$$w^2 - ((4s)^2 + s)v^2 = 8 \tag{4.19}$$

The fundamental solution of

$$w^2 - ((4s)^2 + s)v^2 = 1 \tag{4.20}$$

is $(32s+1, 8)$, and so by Theorem 3.5 for any fundamental solution (W_1, Z_1) of (4.19)

$$0 \leq Z_1 \leq \frac{8\sqrt{2}}{\sqrt{16s+1}}$$

We can rule out $Z_1 = 0$ as this gives $W_1 = \sqrt{8}$, a non-integral solution. By Lemma 4.8, we need not check any s such that $8 < \sqrt{(4s)^2 + s}$ because $\sqrt{8} \notin \mathbb{Z}$.

If $\sqrt{(4s)^2 + s} < 8$, then $s \leq 1$. The following table shows the resulting Pell equation for the various values of s with the possible values of Z_1.

s	Pell Equation	Z_1
1	$w^2 - 17v^2 = 8$	$1, 2$

Since $s = 1$ yields a fundamental solution to (4.19) which turns out to be $(5, 1)$, we are unable to arrive at an immediate contradiction and must directly show that (4.1) has no solutions when $j = 9$ and $k = 66$. Substituting these values gives

$$x^4 - 66x^2y^2 + y^4 = 2^9 \tag{4.21}$$

Suppose (X, Y) is a solution of (4.21). Then

$$\begin{aligned} 2^9 &= (X^4 - 2X^2Y^2 + Y^4) - 64X^2Y^2 \\ &= (X^2 - Y^2)^2 - (8XY)^2 \\ &= [(X^2 - Y^2) - 8XY][(X^2 - Y^2) + 8XY] \end{aligned}$$

and hence, both factors are powers of 2. With the constraints on X and Y by Lemma 4.1, we have

$$(X^2 - Y^2) - 8XY < (X^2 - Y^2) + 8XY$$

so let

$$\begin{aligned} 2^{\alpha} &= (X^2 - Y^2) - 8XY \\ 2^{\beta} &= (X^2 - Y^2) + 8XY \end{aligned} \tag{4.22}$$

with $0 \leq \alpha < \beta \leq 9$ and $\alpha + \beta = 9$. Now

$$16XY = 2^{\beta} - 2^{\alpha} = 2^{\alpha}(2^{\beta-\alpha} - 1)$$

Since $X, Y \in \mathbb{O}$ we have $\alpha = 4$ and thus $\beta = 5$, hence

$$XY = 2^{\beta-\alpha} - 1 = 1$$

Therefore, we are forced to conclude that the only solution of (4.21) is $(1, 1)$. However, this violates Lemma 4.1, and so we have a contradiction. Hence by Lemma 4.1 it follows that there are no nontrivial solutions of (4.17). □

4.6 Case $j = 10$: $x^4 - kx^2y^2 + y^4 = 2^{10}$

We consider the quartic equation

$$x^4 - kx^2y^2 + y^4 = 2^{10} \quad (k \in \mathbb{N}) \tag{4.23}$$

Theorem 4.10. *Equation (4.23) has no nontrivial solutions when $k > 2$ and k is not a square.*

Proof. Suppose that (X, Y) is a solution of (4.23) with $X, Y \in \mathbb{E}$. Let $X = 2U$ and $Y = 2V$. Then (4.23) becomes

$$U^4 - kU^2V^2 + V^4 = 2^6$$

This would imply that (4.1) has a nontrivial solution when $j = 6$, which is a contradiction.

Therefore any solution of (4.23) must be primitive. Since $X, Y \in \mathbb{O}$ for any primtive solution (X, Y) to (4.23), by Corollary 4.6, $k \equiv 2 \pmod{64}$ and so $k = 64s + 2$. Substituting k and j into (4.4) gives the following Pell equation

$$u^2 - (2^{12}s^2 + 2^8 s)v^2 = 2^{12} \tag{4.24}$$

From (4.24) we see that $256|u^2$ and so $16|u$. Letting $u = 16w$ and simplifying (4.24) gives

$$w^2 - ((4s)^2 + s)v^2 = 16 \tag{4.25}$$

The fundamental solution of

$$w^2 - ((4s)^2 + s)v^2 = 1 \tag{4.26}$$

is $(32s+1, 8)$, and so by Theorem 3.5 it follows that for any fundamental solution (W_1, Z_1) of (4.25)

$$0 \leq Z_1 \leq \frac{16}{\sqrt{16s+1}}$$

We can rule out the case where $(W_1, Z_1) = (4, 0)$ because by Lemma 4.7 we have $Z \in \mathbb{E}$ for any solution (W, Z) in the same class as $(4, 0)$. However this is a contradiction since we have assumed that $Y \in \mathbb{O}$ and $Z = Y^2$ implies that $Y \in \mathbb{E}$. By Lemma 4.8, we need not check any s such that $16 < \sqrt{(4s)^2 + s}$ because any solution corresponding to this s is in the same solution class as $(4, 0)$.

If $\sqrt{(4s)^2 + s} < 16$, then $s \leq 3$. The following table shows the resulting Pell equation for the various values of s with the possible values of Z_1.

s	Pell Equation	Z_1
1	$w^2 - 17v^2 = 16$	$1, 2, 3$
2	$w^2 - 66v^2 = 16$	$1, 2$
3	$w^2 - 147v^2 = 16$	$1, 2$

Only $s = 1$ yields a fundamental solution to (4.25), which turns out to be $(13, 3)$. Therefore, we are unable to arrive at an immediate contradiction and must directly show that (4.1) has no solutions when $j = 10$ and $k = 66$. Substituting these values for s and k gives

$$x^4 - 66x^2y^2 + y^4 = 2^{10} \tag{4.27}$$

Suppose (X, Y) is a solution of (4.27). Then

$$\begin{aligned} 2^{10} &= (X^4 - 2X^2Y^2 + Y^4) - 64X^2Y^2 \\ &= (X^2 - Y^2)^2 - (8XY)^2 \\ &= [(X^2 - Y^2) - 8XY][(X^2 - Y^2) + 8XY] \end{aligned}$$

and hence, both factors are powers of 2. With the constraints on X and Y by Lemma 4.1, we have

$$(X^2 - Y^2) - 8XY < (X^2 - Y^2) + 8XY$$

so let

$$\begin{aligned} 2^\alpha &= (X^2 - Y^2) - 8XY \\ 2^\beta &= (X^2 - Y^2) + 8XY \end{aligned} \tag{4.28}$$

with $0 \leq \alpha \leq \beta \leq 10$ and $\alpha + \beta = 10$. Now

$$16XY = 2^\beta - 2^\alpha = 2^\alpha(2^{\beta-\alpha} - 1)$$

Since $X, Y \in \mathbb{O}$ we have $\alpha = 4$ and thus $\beta = 6$, hence

$$XY = 2^{\beta-\alpha} - 1 = 3$$

Therefore, we are forced to conclude that the only solution of (4.27) is $(3, 1)$. However, this solution does not satisfy (4.27). Hence by Lemma 4.1 it follows that there are no nontrivial

solutions of (4.23). □

4.7 Case $j = 11$: $x^4 - kx^2y^2 + y^4 = 2^{11}$

We consider the quartic equation

$$x^4 - kx^2y^2 + y^4 = 2^{11} \quad (k \in \mathbb{N}) \tag{4.29}$$

Theorem 4.11. *Equation (4.29) has no nontrivial solutions when $k > 2$ and k is not a square.*

Proof. Suppose that (X, Y) is a solution of (4.29) with $X, Y \in \mathbb{E}$. Let $X = 2U$ and $Y = 2V$. Then (4.29) becomes

$$U^4 - kU^2V^2 + V^4 = 2^7$$

This would imply that (4.1) has a nontrivial solution when $j = 7$, which is a contradiction. Therefore any solution to (4.29) must be primitive. Since $X, Y \in \mathbb{O}$ for any primtive solution (X, Y) to (4.29), by Corollary 4.6, $k \equiv 2 \pmod{64}$ and so $k = 64s + 2$. Substituting k and j into (4.4) gives the following Pell equation

$$u^2 - (2^{12}s^2 + 2^8 s)v^2 = 2^{13} \tag{4.30}$$

From (4.30) we see that $256|u^2$ and so $16|u$. Letting $u = 16w$ and simplifying (4.30) gives

$$w^2 - ((4s)^2 + s)v^2 = 32 \tag{4.31}$$

The fundamental solution of

$$w^2 - ((4s)^2 + s)v^2 = 1 \tag{4.32}$$

is $(32s+1, 8)$, and so by Theorem 3.5 it follows that for any fundamental solution (W_1, Z_1)

of (4.31)

$$0 \leq Z_1 \leq \frac{16\sqrt{2}}{\sqrt{16s+1}}$$

We can rule out $Z_1 = 0$ as this gives $W_1 = \sqrt{32}$, a non-integral solution. By Lemma 4.8, we need not check any s such that $32 < \sqrt{(4s)^2 + s}$ because $\sqrt{32} \notin \mathbb{Z}$.

If $\sqrt{(4s)^2 + s} < 32$, then $s \leq 7$. The following table shows the resulting Pell equation for the various values of s with the possible values of Z_1.

s	Pell Equation	Z_1
1	$w^2 - 17v^2 = 32$	$1, 2, 3, 4, 5$
2	$w^2 - 66v^2 = 32$	$1, 2, 3$
3	$w^2 - 147v^2 = 32$	$1, 2, 3$
4	$w^2 - 260v^2 = 32$	$1, 2$
5	$w^2 - 405v^2 = 32$	$1, 2$
6	$w^2 - 582v^2 = 32$	$1, 2$
7	$w^2 - 791v^2 = 32$	$1, 2$

Only $s = 1$ yields fundamental solutions to (4.31), which turn out to be $(7, 1)$ and $(10, 2)$. Therefore, we are unable to arrive at an immediate contradiction and must directly show that (4.1) has no solutions when $j = 10$ and $k = 66$. Substituting these values for s and k gives

$$x^4 - 66x^2y^2 + y^4 = 2^{11} \tag{4.33}$$

Suppose (X, Y) is a solution of (4.33). Then

$$\begin{aligned} 2^{11} &= (X^4 - 2X^2Y^2 + Y^4) - 64X^2Y^2 \\ &= (X^2 - Y^2)^2 - (8XY)^2 \\ &= [(X^2 - Y^2) - 8XY][(X^2 - Y^2) + 8XY] \end{aligned}$$

and hence, both factors are powers of 2. With the constraints on X and Y by Lemma 4.1,

we have

$$(X^2 - Y^2) - 8XY < (X^2 - Y^2) + 8XY$$

so let

$$\begin{aligned} 2^\alpha &= (X^2 - Y^2) - 8XY \\ 2^\beta &= (X^2 - Y^2) + 8XY \end{aligned} \tag{4.34}$$

with $0 \leq \alpha < \beta \leq 11$ and $\alpha + \beta = 11$. Now

$$16XY = 2^\beta - 2^\alpha = 2^\alpha(2^{\beta-\alpha} - 1)$$

Since $X, Y \in \mathbb{O}$ we have $\alpha = 4$ and thus $\beta = 7$, hence

$$XY = 2^{\beta-\alpha} - 1 = 7$$

Therefore, we are forced to conclude that the only solution of (4.33) is $(7, 1)$. However, this solution does not satisfy (4.33). Hence by Lemma 4.1 it follows that there are no nontrivial solutions of (4.29). □

Future Work

We would like to see these methods extended in order to solve more cases of j. In order to do this, we need a more thorough investigation of the family of Pell equations

$$x^2 - ((4s)^2 + s)v^2 = 2^r$$

when $\sqrt{(4s)^2 + s} < 2^r$. Our hope is that only

$$x^2 - 17v^2 = 2^r$$

will yield a fundamental solution, in which case we are confident that we can generalize the previous arguments to show that

$$x^4 - 66x^2y^2 + y^4 = 2^j$$

has no nontrivial solutions for all j.

Bibliography

[1] A. Agarwal, *Some Quartic Diophantine Equations*, Ph.D. thesis, SUNY Buffalo, 2005.

[2] D. Burton, *Elementary Number Theory*, 6th ed., Mc Graw Hill, New York, 2007.

[3] S.C. Coutinho, *The Mathematics of Ciphers: Number Theory and RSA Cryptography*, A K Peters, Massachusetts, 1999.

[4] A. Dujella, *Continued fractions and RSA with small secret exponent*, Tatra Mt. Math. Publ. **29** (2004), 101–112.

[5] J. Hoffstein, J. Pipher, and J.H. Silverman, *An Introduction to Mathematical Cryptography*, Springer, New York, 2008.

[6] I. Niven, H.S. Zuckerman, and H.L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., John Wiley & Sons, New York, 1991.

[7] M.J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Trans. Inform. Theory **36** (1990), 553–558.