Integer Solutions to the Equation $a^n + b^n = c^n$ for $n > 2$

John Halloran
Department of Mathematics

1 Introduction

In this paper, we will derive integer solutions to

$$a^n + b^n = c^n$$

for the cases $n = 2$ and $n = 4$. We will also briefly describe the math involving elliptic curves and present a short outline of the proof for Fermat’s Last Theorem, the general solution for $n > 2$. 
2 The case \( n = 2 \)

For \( n = 2 \), we have the equation

\[
a^2 + b^2 = c^2.
\]  

(2)

A Pythagorean Triple is a set of integers \((a, b, c)\) which satisfy equation 2. Notice that if \( a, b, \) and \( c \) share a common divisor, we may simplify the Pythagorean Triple by factoring out this divisor. A Primitive Pythagorean Triple (PPT) is a Pythagorean Triple in which \( a, b, \) and \( c \) are relatively prime. The first few PPT’s are displayed in table 1. Given any Pythagorean Triple, we may obtain an infinite number of Pythagorean Triples by multiplying equation (2) by a constant. However, how many unique PPT’s exist? We now prove several important properties of PPT’s to answer this question.

\[
\begin{array}{|c|c|c|}
\hline
a & b & c \\
\hline
3 & 4 & 5 \\
5 & 12 & 13 \\
7 & 24 & 25 \\
9 & 40 & 41 \\
15 & 8 & 17 \\
21 & 20 & 29 \\
35 & 12 & 37 \\
45 & 28 & 53 \\
\hline
\end{array}
\]

Table 1: First 7 PPT terms, increasing in order of \( a \).

**Proposition.** For a given PPT \((a, b, c)\), \( c \) is always odd and either \( a \) is odd and \( b \) is even, or \( a \) is even and \( b \) is odd.

**Proof.** Assume that \( a \) and \( b \) are even. Then \( c \) must also be even. Thus, \( a, b, \) and \( c \) share the common divisor 2. However, \((a, b, c)\) is a PPT, and \( \gcd(a, b, c) = 1 \). \( \Rightarrow \) Therefore, \( a \) and \( b \) cannot both be even.

Next, assume \( a \) and \( b \) are both odd. The squares of \( a \) and \( b \) must also be odd, so their sum
must be even, and \( c \) must be even. Thus, \( a = 2n + 1 \), \( b = 2m + 1 \), \( c = 2l \) for some \( n, m, l \in \mathbb{Z} \), so

\[
\begin{align*}
(2n + 1)^2 + (2m + 1)^2 &= 4l^2 \\
4n^2 + 4n + 1 + 4m^2 + 4m + 1 &= 4l^2 \\
4(n^2 + m^2 + n + m) + 2 &= 4l^2 \\
2(n^2 + m^2 + n + m) + 1 &= 2l^2
\end{align*}
\]

The term on the left is odd while the term on the right is even, which is impossible. \( \Rightarrow \Leftarrow \)

Therefore, \( a \) and \( b \) cannot both be odd.

Thus, one of \( a, b \) must be even while the other is odd. From this result, we know \( c \) is odd. \( \square \)

Next, consider solving for \( a^2 \) in equation (2). We have the following

\[ a^2 = c^2 - b^2 = (c + b)(c - b) \quad (3) \]

Taking the \( a \) terms from table 1 and squaring them, we have

\[
\begin{align*}
3^2 &= 9 \cdot 1 \\
5^2 &= 25 \cdot 1 \\
7^2 &= 49 \cdot 1 \\
9^2 &= 81 \cdot 1 \\
15^2 &= 9 \cdot 25 \\
21^2 &= 9 \cdot 49 \\
35^2 &= 25 \cdot 49 \\
45^2 &= 25 \cdot 81
\end{align*}
\]

While the first few terms are a bit trivial, it looks as though \( a^2 \) is always a product of two squares, and so we make the following proposition.

**Proposition.** For a given PPT, \( (c-b) \) and \( (c+b) \) are squares.

**Proof.** We first prove that \( (c-b), (c+b) \) are relatively prime. Assume that \( d | (c+b), d | (c-b) \),
for some $d \in \mathbb{Z}$. Then, $c - b = md$, $c + b = nd$ for some $n, m \in \mathbb{Z}$, and
\[
\begin{align*}
md - nd & = (c + b) - (c - b) \\
d(m - n) & = 2b \\
m - n & = \frac{2b}{d}
\end{align*}
\]
where $(m - n) \in \mathbb{Z}$, so $d|2b$. Similarly,
\[
\begin{align*}
md + nd & = (c + b) + (c - b) \\
d(m + n) & = 2c \\
m - n & = \frac{2c}{d}
\end{align*}
\]
$(m + n) \in \mathbb{Z}$, so $d|2c$. By definition, $b$ and $c$ are relatively prime, so either $d = 2$ or $d = 1$. However, $d$ must also divide $a$, and $a$ is odd, so $d$ must be 1. Thus, $(c + b)$ and $(c - b)$ are relatively prime.

Now, let $(c - b) = j$ and $(c + b) = k$, for some $j, k \in \mathbb{Z}$. Thus, $jk = a^2$; however, we just proved that $j$ and $k$ are relatively prime, so this can only be true if $j$ and $k$ are squares themselves. Thus, we have $j = s^2, k = t^2$ for some $s, t \in \mathbb{Z}$ such that $gcd(s, t) = 1$. Thus, $(c - b) = s^2$ and $(c + b) = t^2$.

We use our results to obtain the following:
\[
\begin{align*}
(c - b)(c + b) & = a^2 \\
s^2t^2 & = a^2 \\
(st)^2 & = a^2 \\
st & = a
\end{align*}
\]
Notice that $a$ is odd, and so both $s$ and $t$ must be odd. We now solve for $c$ and $b$ in terms of $s$ and $t$:
\[
\begin{align*}
(c + b) + (c - b) & = t^2 + s^2 \\
2c & = t^2 + s^2 \\
c & = \frac{t^2 + s^2}{2}
\end{align*}
\]
\[(c + b) - (c - b) = t^2 - s^2\]
\[2b = t^2 - s^2\]
\[b = \frac{t^2 - s^2}{2}\]

Thus, every PPT \((a, b, c)\) is of the following form:

\[a = st, \quad b = \frac{t^2 - s^2}{2}, \quad c = \frac{t^2 + s^2}{2}\]

where \(s, t\) are odd and relatively prime integers. There are infinitely many relatively prime numbers \(s\) and \(t\), so there are infinitely many PPT’s. We now shift our attention to \(n\) greater than 2.

3 The case \(n > 2\)

For \(n > 2\), we have the following Theorem:

**Fermat’s Last Theorem.**

\[a^n + b^n = c^n\]

has no integer solutions for \(n > 2\).

This particular theorem is well-known around the world. We now briefly discuss the history of this theorem and what approach we will take to attempt to solve it.

3.1 A note in the Margin

Pierre de Fermat (1605-1665) was a French lawyer who engaged in mathematics to pass the time. He is typically accredited with the birth of modern number theory. However, he was not a professional mathematician. He only published a single mathematical paper. Most of his work survived through his copy of Diophantus’ *Arithmetica*, in which he would work
through problems and write his mathematical findings in the margins of the book’s pages. In one margin, he wrote:

It is impossible for a cube to be written as a sum of two cubes or a fourth power to be written as the sum of two fourth powers or, in general, for any number which is a power greater than the second to be written as a sum of two like powers.

This became what we now call Fermat’s Last Theorem (which we will denote as FLT). This conjecture is widely regarded as one of the most difficult math problems in history. Mathematicians could neither prove nor disprove it for over 350 years. However, what really drove people mad was what Fermat wrote directly after:

I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain.

Fermat claimed to have had an elegant proof of the FLT, which he could not fit in the margin. So where was this proof? Fermat never wrote it down! Although Fermat claimed to have proved the FLT, there is no evidence which supports this claim. People today are very skeptical that Fermat had a correct proof. However, he is accredited with the proof of the FLT for $n = 4$, although he only described a general method to solve the case $n = 4$ and did not provide the actual proof nor the details of the method. This method was eventually re-discovered by Leonard Euler (1707-1783) and is now known as Fermat’s Method of Infinite Descent.

### 3.2 Proving Fermat’s Last Theorem

How do we go about proving or disproving the FLT? We begin by noting that if $n = mp$, then equation 1 becomes

$$a^{mp} + b^{mp} = c^{mp}$$

$$\left(a^m\right)^p + \left(b^m\right)^p = \left(c^m\right)^p \quad (6)$$
So, if there are no integers which satisfy equation 1 for \( n = p \), then there are also no integer solutions to equation 6. Thus, if we can prove the FLT for \( p \), then the FLT is true for all multiples of \( p \). This means we need only prove the FLT for all odd primes and \( n = 4 \), which greatly reduces our task since we do not have to arbitrarily prove the FLT for every number \( n > 2 \). We now set out to prove the FLT for \( n = 4 \) and, consequently, every multiple of 4.

4  The case \( n = 4 \)

Let \( n = 4 \). Then equation 1 becomes

\[
a^4 + b^4 = c^4. \tag{7}
\]

We can factor out any common divisor of \( a, b \) and \( c \), so assume that \( a, b, c \) are relatively prime. From equation 7 we notice the following

\[
a^4 + b^4 = (c^2)^2.
\]

This tells us that in order for a fourth power to be the sum of two fourth power, it must first be true that a square may be the sum of two fourth powers. We will prove the stronger case, that a square cannot be the sum of two fourth powers. To prove this, we will assume that the FLT is false, that is, that there does exist a square which is the sum of two fourth powers, then hopefully find a contradiction to this assumption.

**Modified Fermat’s Last Theorem for \( n = 4 \).** There do not exist non-trivial integers \((a, b, c)\) which satisfy

\[
a^4 + b^4 = c^2. \tag{8}
\]

Proof. Assume \( \exists \) non-zero integers \((a, b, c)\) which satisfy equation 8, and \( \gcd(a, b, c) = 1 \). Let \( x^2 = a, y^2 = b, \) and \( z = c \). Then equation 8 becomes

\[
x^2 + y^2 = z^2.
\]

Further, \( x, y, \) and \( z \) must be relatively prime, so we now have a PPT. From our work in section 2, we know \((x, y, z)\) must be of the form

\[
a^2 = x = st \tag{9}
\]
\[
b^2 = y = \frac{t^2 - s^2}{2} \tag{10}
\]
\[
c = z = \frac{t^2 + s^2}{2} \tag{11}
\]
where $s$ and $t$ are odd, relatively prime integers. Also, $b^2$ is positive, so we must make the restriction that $t > s$. Equation 10 tells us that

$$
2b^2 = t^2 - s^2 \\
2b^2 = (t - s)(t + s)
$$

Assume that $(t - s)$ and $(t + s)$ share a common factor, $d$. Then $(t - s) = md$ and $(t + s) = nd$, for some $n, m \in \mathbb{Z}$. By adding and subtracting the two, we have

$$
2s = d(m + n) \\
2t = d(m - n)
$$

Thus, $d$ must divide both $2s$ and $2t$. However, $gcd(s, t) = 1$, so either $d = 2$ or $d = 1$. From equation 12, $d$ must also divide $2b^2$, so $d = 2$. Thus, we have $(t - s) = 2m$, $(t + s) = 2n$. Substituting this into equation 12, we have

$$
2b^2 = (2m)(2n) \\
b^2 = 2mn \\
b = \sqrt{2mn}
$$

Thus $m$ and $n$ must be squares. However, from equation 13, either $m$ or $n$ must have an extra factor of 2. We will take the convention that $m$ carries the extra factor of 2. Thus, we have $m = 2v^2$, $n = u^2$ for some $u, v \in \mathbb{Z}$, and $(t - s) = 4v^2$, $(t + s) = 2u^2$. Further, $gcd(t - s, t + s) = 2$, so $u$ and $v$ must be relatively prime. Solving for $s$ and $t$ in terms of $u$ and $v$ yields

$$
s = 2v + u^2 \\
t = u^2 - 2v^2
$$

From equation 9,

$$
a^2 = st \\
= (2v + u^2)(u^2 - 2v^2) \\
= u^4 - 4v^2
$$

Rearranging this equation gives us

$$
u^4 = a^2 + 4v^2. \tag{13}
$$

Now, let $A = a$, $B = 2v^2$, $C = u^2$. Then from equation 13, we have

$$
A^2 + B^2 = C^2 \tag{14}
$$
where \(A, B, C\) are relatively prime. Thus, we have another PPT, which means that \(A, B, C\) must be of the form

\[
\begin{align*}
a &= A = ST \\ 2v^2 &= B = \frac{T^2 - S^2}{2} \\ u^2 &= C = \frac{T^2 + S^2}{2}
\end{align*}
\]  

(15)

(16)

(17)

where \(T\) and \(S\) are integers such that \(T > S\) and \(\gcd(T, S) = 1\). From equation 16

\[4v^2 = T^2 - S^2 = (T + S)(T - S).\]  

(18)

As we proved with equation 12, \(\gcd(T - S, T + S) = 2\). Performing similar calculations as we did with equation 12, we have

\[
\begin{align*}
T + S &= 2X^2 \\
T - S &= 2Y^2
\end{align*}
\]

for relatively prime integers \(X\) and \(Y\). Thus,

\[
\begin{align*}
T &= X^2 + Y^2 \\
S &= X^2 - Y^2
\end{align*}
\]

Plugging these into equation 17, we have the following

\[
u^2 = \frac{T^2 + S^2}{2} = \frac{(X^2 + Y^2)^2 + (X^2 - Y^2)^2}{2} = \frac{X^4 + 2X^2Y^2 + Y^4 + X^4 - 2X^2Y^2 + Y^4}{2} = \frac{2(X^4 + Y^4)}{2} = X^4 + Y^4
\]

where \(u, X, Y\) are relatively prime. Thus, we have a new set of integers which satisfy equation 8. Further, if we trace back through our calculations,

\[
z^2 = \frac{s^2 + t^2}{2} = \frac{(u^2 + 2v^2) + (u^2 - 2v^2)^2}{2} = u^2 + 4v^2
\]
so \( u^2 < z^2 \). Thus, our new solution to equation 8 is smaller than our original solution. Now that we have our new solution to equation 8, we will apply exactly the same calculations we just did to our original solution. In this manner, we find another set of integers \((u_2, X_2, Y_2)\) which satisfy equation 8. Further, this set of integers will also be relatively prime, so we produce yet another set of integers \((u_3, X_3, Y_3)\) which satisfy equation 8. We cannot stop ourselves now. Each new set of integers we produce which solve equation 8 are relatively prime, thus, we must apply the same procedure to it (descend upon it) and use it to find another set of integers which satisfy 8. Thus, in this manner, we produce infinitely many integer solutions to equation 8. Further, each new square which we find to be the sum of two fourth powers is smaller than the previous square found to be the sum of two fourth powers. Thus, our infinite list looks like

\[
\begin{align*}
  u^2 &< z^2 \\
  u_2^2 &< u^2 \\
  u_3^2 &< u_2^2 \\
  u_4^2 &< u_3^2 \\
  u_5^2 &< u_4^2 \\
  &\vdots
\end{align*}
\]

However, this is an infinite list of positive, decreasing integers, and by the Well-Ordering Principle this is impossible. \( \Rightarrow \Leftarrow \) Thus, \( \# \) non-zero integers which satisfy equation 8.

So in the integers, no square may be the sum of two fourth powers, and subsequently, no fourth power may be the sum of two fourth powers. Thus, the FLT is true for \( n = 4 \). The method we just used to prove the Modified FLT for \( n = 4 \) was Fermat’s Method of Infinite Descent, the technique we discussed in section 3.1. To summarize this technique, one assumes that there exists a solution to a particular equation, then uses this assumption to generate an infinite list of positive decreasing integers, which is impossible.

\section{5 A Need for Modern Tools}

We have just proved the FLT for \( n = 4 \), and thus for all multiples of 4 (as we discussed in section 3.2). This is a very powerful result, proving the FLT for infinitely many numbers. We could carry on proving the FLT for each odd prime. However, there are infinitely many
odd primes (and only one even prime). Further, many odd primes involve proving the FLT with different methods. We need something that proves the FLT for all odd primes, all at once. Thus, we must look towards more modern mathematics to prove the FLT for all odd primes in a single stroke. We must look at the math surrounding elliptic curves.

6 Elliptic Curves

6.1 Definition of an Elliptic Curve

Consider an equation of the form

\[ E : y^2 = x^3 + ax^2 + bx + c \]  \hspace{1cm} (19)

where \( E \) denotes the curve of the equation. We will restrict \( y, x, a, b, \) and \( c \) to be integers. \( E \) is said to be an elliptic curve if its discriminant is non-zero, where the discriminant is defined as

\[ \Delta(E) = -4a^3 + a^2b^2 - 4b^3 - 27c^2 + 18abc. \]  \hspace{1cm} (20)

The following plots are examples of several different elliptic curves. Things to note are when the discriminant of a curve is negative, the curve is a single segment as in figures 1 and 3, and when the discriminant is positive, the curve is comprised of two segments as in figure 2. Also, notice that an elliptic curve is always symmetrical about the \( x \)-axis. A curve \( E \) with \( \Delta(E) = 0 \) intersects itself at what is called a singularity point. Thus, we require elliptic curves to have a non-zero determinant to ensure the curve is non-singular.
Figure 1: $E : y^2 = x^3 - x + 1, \Delta(E) = -23$

Figure 2: $E : y^2 = x^3 - x, \Delta(E) = 4$
6.2 The Addition Operation for Elliptic Curves

We now define the addition operation on elliptic curves, denoted by '+':

**Definition** Let $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$ be points on an elliptic curve $\exists x_P \neq x_Q$. Define $s = \frac{(x_P - x_Q)}{(x_P - x_Q)}$ and $R = P + Q = (x_R, y_R)$, where $y_R = -y_P + s(x_P - x_R)$.

Then:

(i) if $x_P = x_Q$, we have the following:

1. If $y_P = -y_Q$, then $P + Q = 0$.
2. If $y_P = y_Q \neq 0$, then $R = P + P = 2P = (x_R, y_R)$, where

$$s = \frac{(3x_P^2 - P)}{2y_P}, \quad x_R = s^2 - 2x_P, \quad y_R = -y_P + s(x_P - x_R)$$

(ii) if $y_P = y_Q = 0$, then $P + P = 0$. 

Figure 3: $E : y^2 = x^3 + x$, $\Delta(E) = -4$
The addition operation gives a method to find a new point on the curve using two known points. Thus, we find new solutions to the equation of the curve using known solutions. We now look at a geometric interpretation of the addition operation, using the curve from figure 1 as a reference. Under the addition operation, we are guaranteed to obtain three points on the curve by drawing a non-horizontal line through any two points. Further, these three points will always add up to 0. In figure 4, we have a line passing through the points $P, Q$, and $R$, where $R$ is defined as the inverse of $P + Q$. Thus, we have

$$P + Q + R = P + Q - (P + Q) = 0$$

We define a point at infinity for any vertical line drawn on an elliptic curve. Further, this point at infinity is defined to be the identity, 0, under +. Due to the symmetry of an elliptic curve, any point on the curve which a vertical line passes through will have its inverse on the same point of the curve opposite the x-axis. Thus, from figure 5, we have

$$P + (-P) + 0 = P - P = 0$$

Figure 6 displays the case when the line passes through a point tangent to the curve. Notice that we only have two points on the line passing through the curve. Thus, when a line passes through $P$, a point tangent to the curve, we consider the line to pass through $P$ twice. This is known as the doubling principal. When this happens, $R$ is defined to be the inverse of $2P$, and so we have

$$P + P + R = 2P - 2P = 0$$

Figure 7 displays the case when a vertical line passes through a point tangent to the curve. In this case, we must use the doubling principal and the point at infinity 0. Also, notice that $P$ is its own inverse due to the symmetry of the curve, so

$$2P + 0 = P \cdot P = 0$$

These four are the only possible cases to construct a line through two points on an elliptic curve under the addition operation.
Figure 4: Line passing through 3 points on the curve.

Figure 5: Point at infinity and inverses due to symmetry of the curve.
Figure 6: Line passing through a point tangent to the curve: the doubling principal.

Figure 7: Vertical line passing through a point tangent to the curve.
Also, it can be shown, as in [3], that any elliptic curve $E$ under $+$ has the following properties: Let $P, Q,$ and $R$ be points on $E$. Then

1. $+$ is well-defined on $E$.
2. $\exists$ an identity, $0$, on $E \ni P + 0 = 0 + P = P$.
3. All points on $E$ have an inverse under $+$.
4. $(P + Q) + R = P + (R + Q)$
5. $P + Q = Q + P$

$\therefore$ Every elliptic curve under $+$ form an Abelian Group.

Now, we have a basic understanding of elliptic curves. However, what does this have to do with Fermat’s Last Theorem?

## 7 A Bridge Between Fermat’s Last Theorem and Elliptic Curves

In 1984, Gerhard Frey proved the following:

Assume that for $p$ an odd prime, a set of integers $(a, b, c)$ exist which satisfy

$$a^p + b^p = c^p.$$  

Then the following elliptic curve must also exist

$$y^2 = x(x - a^p)(x + b^p).$$  \hspace{1cm} (21)

Equation 21 is now known as Frey’s Curve. Notice that for Frey’s Curve to exist, the FLT must be false. Further, Kenneth Ribet proved that Frey’s Curve could not be modular (which was called the Epsilon Conjecture). However, the Tayinama-Shimura Conjecture states that every elliptic curve must be modular. Thus, if one could prove the Tayinama-Shimura Conjecture, then Frey’s Curve could not exist, and thus, the FLT would be true. At the same time, if someone could show that Frey’s Curve did exist, than this would mean the FLT was false.
To explain what it means for an elliptic curve to be modular, assume that we are looking for solutions modulo $p$ to the curve, where $p$ is a prime. As an example, take the curve from figure 3,

$$E : y^2 = x^3 + x.$$  \hspace{1cm} (22)

The first few modular solutions to equation 22 are in table 2, where $N_p$ is the number of solutions modulo $p$. The quantity $p - N_p$ is known as the $p$-defect of the curves, and the list of $p$-defects is known as the $L$-Series of the curve. An elliptic curve is said to be modular if there exists a function, known as the $L$-function of $E$, which encapsulates all values of the $L$-Series within it. Such a function looks like

$$L(E, s) = \prod_p \left(1 - \frac{a_p}{p^2} + \frac{1}{p^{2s-1}}\right)^{-1}$$

where $p$ is a prime and $a_p = p - N_p$. Also, an elliptic curve is said to be semistable if a prime divides its discriminant.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$N_p$</th>
<th>$p - N_p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>19</td>
<td>-6</td>
</tr>
<tr>
<td>17</td>
<td>15</td>
<td>2</td>
</tr>
<tr>
<td>19</td>
<td>19</td>
<td>0</td>
</tr>
<tr>
<td>23</td>
<td>23</td>
<td>0</td>
</tr>
<tr>
<td>29</td>
<td>19</td>
<td>10</td>
</tr>
<tr>
<td>31</td>
<td>31</td>
<td>0</td>
</tr>
<tr>
<td>37</td>
<td>35</td>
<td>2</td>
</tr>
<tr>
<td>41</td>
<td>31</td>
<td>10</td>
</tr>
</tbody>
</table>
8 The FLT in One Fell Swoop

In 1994, Andrew Wiles managed to prove a special case of the Tayanama-Shimura Conjecture, that every semistable elliptic curve must be modular. It turns out that Frey’s Curve is semistable. So, Andrew Wiles proved that Frey’s Curve must be modular, but Kenneth Ribet proved that it cannot be modular.⇒⇐
∴ Frey’s Curve cannot exist.
∴ ∄ non-zero integers which satisfy equation 1 for \( n = p \), an odd prime. Thus, Fermat’s Last Theorem is true.

9 Conclusion

Andrew Wiles’ proof of a special case of the Tayanama-Shimur Conjecture was no small feat. Once word of Kenneth Ribet’s proof that Frey’s Curve could not be modular went around, Wiles went into seclusion for 6 years, developing his own methods to prove that every semistable elliptic curve was modular. He is accredited with the proof of Fermat’s Last Theorem, with partial credit going to Richard Taylor and Kenneth Ribet. Wiles proof is usually regarded as one of the greatest achievements of modern mathematics, combining some of the hardest mathematics in the world as well as developing his own breakthrough mathematical techniques.

References


