Rose-Hulman Undergraduate Mathematics Journal

Volume 13
Issue 1

Article 3

A Factorial Power Variation of Fermat's Equation

Matthew J. Green
Towson University, mgreen30@students.towson.edu

Rose-Hulman Undergraduate Mathematics Journal

A factorial power variation of Fermat's equation

Matthew J. Green[a]

Volume 13, No. 1, Spring 2012

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
Email: mathjournal@rose-hulman.edu
http://www.rose-hulman.edu/mathjournal

[a]Towson University, mgreen11110@gmail.com

Rose-Hulman Undergraduate Mathematics Journal
Volume 13, No. 1, Spring 2012

A factorial power variation of Fermat's equation

Matthew J. Green

Abstract. We consider a variant of Fermat's well-known equation $x^n + y^n = z^n$. This variant replaces the usual powers with the factorial powers defined by $x^{\underline{n}} = x(x-1)\cdots(x-(n-1))$. For $n = 2$ we characterize all possible integer solutions of the equation. For $n = 3$ we show that there exist infinitely many non-trivial solutions to the equation. Finally we show there exists no maximum n for which $x^{\underline{n}} + y^{\underline{n}} = z^{\underline{n}}$ has a non-trivial solution.

Acknowledgements: The author would like to thank Dr. A. Kolesnikov for his support and guidance during this research, as well as Dr. A. Kumchev and the anonymous referee for their review and ideas which helped increase the quality of this paper.

1 Introduction

The search for solutions to the Diophantine equation $x^n + y^n = z^n$ has lead to the well-known Pythagorean triples as well as Fermat's last conjecture, which was eventually proven by Andrew Wiles [1]. Over the years a number of variations of this equation have also been considered, such as replacing the integral powers with rational powers (see [2] [3]). We consider a variation that replaces the nth powers with the factorial powers. That is, we consider the equation

$$x^{\underline{n}} + y^{\underline{n}} = z^{\underline{n}}, \tag{1}$$

where the factorial power, $x^{\underline{n}}$, is defined by Graham, Knuth, and Patashnik [5] as follows.

Definition 1.1. Let x be a real number and $n \geq 1$ be an integer. The *factorial power n of x*, denoted $x^{\underline{n}}$, is defined by the formula,

$$x^{\underline{n}} = x(x-1)\cdots(x-n+1).$$

The standard form of the equation has infinitely many solutions for $n = 2$, and no non-trivial solutions for $n > 2$. We will show that the factorial power variation has infinitely many non-trivial solutions for $n = 2$ and $n = 3$, and that non-trivial solutions exist for arbitrarily large values of n.

In Section 1 we will be introducing a few tools that will be of use throughout our work, as well as noting the trivial solutions. In Section 2 we completely describe all integral solutions to the equation for $n = 2$. Following this, we show that there exists infinitely many solutions for $n = 3$ in Section 3, and conclude our investigation in Section 4 with a proof that there exists no maximum n for which non-trivial solutions exist.

2 General Observations

The main object of study of this paper is equation (1), and throughout the paper it will be assumed that x, y, and z are integers.

Clearly for non-negative integers less than n we have $x^{\underline{n}} = 0$. As such, if y is less than n, we have a trivial solution $x^{\underline{n}} + y^{\underline{n}} = z^{\underline{n}} + 0 = x^{\underline{n}}$ for any integer x.

At this time we will note that the even factorial powers are symmetric, and the odd factorial powers are antisymmetric, around $\frac{n-1}{2}$.

Claim 2.1. *For all x, we have $x^{\underline{n}} = (-1)^n(n-x-1)^{\underline{n}}$.*

Proof. Expanding $x^{\underline{n}}$, we have

$$\begin{aligned} x^{\underline{n}} &= x(x-1)\cdots(x-n+1) \\ &= (-1)^n(-x)(-x+1)\cdots(-x+n-1) = (-1)^n(n-x-1)^{\underline{n}}. \end{aligned}$$

□

This leads us to note another set of trivial solutions for odd n. If $y = -(n - x - 1)$ then $x^{\underline{n}} + y^{\underline{n}} = 0$, and thus z can be any positive integer less then n.

Additionally, the definition of the factorial powers leads us directly to another simple solution for each n, which we will consider trivial. Setting $x = y = 2n - 1$ we have

$$\begin{aligned}(2n-1)^{\underline{n}} + (2n-1)^{\underline{n}} &= 2(2n-1)(2n-2)\cdot \ldots \cdot n \\ &= 2n(2n-1)\cdot \ldots \cdot (n+1) = (2n)^{\underline{n}}.\end{aligned}$$

Thus for all n, we have the solution $(2n-1)^{\underline{n}} + (2n-1)^{\underline{n}} = (2n)^{\underline{n}}$.

As such we will use the following definition of trivial solutions through out this paper.

Definition 2.2. Any solution to equation 1 such that x, y, or z is non-negative and less then n, or $x = y = 2n - 1$, will be considered *trivial*.

Note that, the binomial coefficients can be defined as follows:

$$\binom{x}{n} = \frac{x^{\underline{n}}}{n!}.$$

From this we can see that $x^{\underline{n}} + y^{\underline{n}} = z^{\underline{n}}$ if and only if

$$\binom{x}{n} = \binom{z}{n} - \binom{y}{n}. \tag{2}$$

3 Factorial Squares

For the case of $n = 2$ we will assume for simplicity that $x \geq 2$ and $y < z$ as the remaining solutions are either trivial or can be obtained using Claim 2.1. We will begin by considering the equation (2). In this case we have $\binom{x}{2} = \sum_{j=0}^{x-1} j$, which leads us to the following claim.

Claim 3.1. *A triple (x, y, z) is a solution to the equation $x^{\underline{2}} + y^{\underline{2}} = z^{\underline{2}}$ if and only if $\binom{x}{2} = \sum_{j=y}^{z-1} j$.*

Proof. From equation (2), we obtain

$$\binom{x}{2} = \binom{z}{2} - \binom{y}{2} = \sum_{j=y}^{z-1} j.$$

□

Note that by defining the binomial coefficients in terms of the factorial powers in the end of Section 2, we have extended the binomial coefficients to the negative integers. Thus $\binom{x}{2}$ is the sum of m consecutive integers if and only if there exists some y and z, whose difference is m, such that $x^{\underline{2}} = z^{\underline{2}} - y^{\underline{2}}$. This leads us to the following claim.

Claim 3.2. *Let N be an integer and m be a positive integer. Then N is the sum of m consecutive integers if and only if m divides $2N$ and either m or $\frac{2N}{m}$ is odd.*

Proof. Clearly, N is the sum of m consecutive integers if and only if there exists a y such that

$$2N = 2\left(ym + \frac{m(m-1)}{2}\right) = m(2y + m - 1). \tag{3}$$

Thus we see that m divides $2N$.

If m is even, then as $2N = m(2y+m-1)$, we see that m divides $2N$ and, as $2y$ is clearly even, $2y + m - 1 = \frac{2N}{m}$ is odd.

From the above equalities it is clear the converse also holds. □

Now we have a full description of how a given number can be written as the sum of consecutive integers. With this we can describe all integer solutions to equation (1) for the case of $n = 2$.

We will introduce the following set to first allow us to clearly describe all solutions for a given x, and then to allow us to extend this to describe all solutions for a given m.

Definition 3.3. For a given integer x, let $\mathcal{D}(x)$ be the set of odd divisors of x.

Now we have the following theorem describing all solutions containing x as a summand, with $z > 0$.

Theorem 3.4. *Let x be a positive integer. Each integer solution (y, z) to the equation*

$$x^{\underline{2}} + y^{\underline{2}} = z^{\underline{2}} \tag{4}$$

with $z > 0$, belongs to one of two disjoint families of solutions, ϕ_x and ψ_x, parameterized by the odd divisors of $x^{\underline{2}}$ as follows:

$$\phi_x = \left\{ \left(\frac{q + q^2 - x^{\underline{2}}}{2q}, \frac{q + q^2 + x^{\underline{2}}}{2q} \right) : q \in \mathcal{D}(x^{\underline{2}}) \right\},$$

$$\psi_x = \left\{ \left(\frac{q - q^2 + x^{\underline{2}}}{2q}, \frac{q + q^2 + x^{\underline{2}}}{2q} \right) : q \in \mathcal{D}(x^{\underline{2}}) \right\}.$$

Proof. Let x be a positive integer, and (y, z) be an integer solution to equation (4). Then, by Claim 3.1 we have that $\binom{x}{2}$ must be the sum of m consecutive integers, where $m = z - y$. By Claim 3.2, we have that m divides $x^{\underline{2}}$ and either m or $d = \dfrac{x^{\underline{2}}}{m}$ is odd. For a given odd divisor q of $x^{\underline{2}}$ we have that either $q = m$ or $q = d$. If $q = m$ by equation (3) we have $y = \dfrac{x^{\underline{2}} - m^2 + m}{2m}$. Therefore $z = \dfrac{x^{\underline{2}} + m^2 + m}{2m}$ and we have $(y, z) \in \psi_x$. Similarly if $q = d$ it is easy to check that $(x, y) \in \phi_x$.

Note that, by the construction of the sets and Claim 3.2, all elements of ψ_x will be integer solutions to equation (4), and the same holds for all elements ϕ_x.

Due to the parity of m the sets are clearly disjoint. □

From this theorem and Claim 2.1 we have the following corollary.

Corollary 3.5. *For each integer x, there exists $4d$ distinct solutions to equation (4) which include x in the summand, where d is the number of odd divisors of $x^{\underline{2}}$.*

Example 3.6. To obtain all solutions which include 28 as a member of the summand, we start with the set $\mathcal{D}(28^{\underline{2}}) = \{1, 3, 7, 9, 21, 27, 63, 189\}$.

From Theorem 3.4, we obtain the sets ψ_{28} and ϕ_{28}, and from these sets of solutions, applying Claim 2.1 to z for each member provides the remaining solutions which include 28 as shown below.

q	ϕ_{28}	ψ_{28}	Related Solutions	
1	$(-377, 379)$	$(378, 379)$	$(-377, -378)$	$(378, -378)$
3	$(-124, 128)$	$(125, 128)$	$(-124, -127)$	$(125, -127)$
7	$(-50, 58)$	$(51, 58)$	$(-50, -57)$	$(51, -57)$
9	$(-37, 47)$	$(38, 47)$	$(-37, -46)$	$(38, -46)$
21	$(-7, 29)$	$(8, 29)$	$(-7, -28)$	$(8, -28)$
27	$(0, 28)$	$(1, 28)$	$(0, -27)$	$(1, -27)$
63	$(26, 38)$	$(-25, 38)$	$(26, -37)$	$(-25, -37)$
189	$(93, 97)$	$(-92, 97)$	$(93, -96)$	$(-92, -96)$

Thus giving us all 32 solutions including 28 in the summand.

As the parameter m has been so important in providing this solution, we will conclude our examination of the solutions for $n = 2$ with a description of our solution set based on m.

Corollary 3.7. *Let m be an integer. If $m = 2k+1$, then the set all triples of falling factorial power 2 such that $z - y = m$ can be written as*

$$x^{\underline{2}} + \left(\frac{x^{\underline{2}} - m^2 + m}{2m}\right)^{\underline{2}} = \left(\frac{x^{\underline{2}} + m^2 + m}{2m}\right)^{\underline{2}},$$

where x is an integer such that $m \in \mathcal{D}(x^{\underline{2}})$.

If $m = 2r$, then all triples of falling factorial power 2 such that $z - y = m$ can be written as

$$x^{\underline{2}} + \left(\frac{m^2 - x^{\underline{2}} + m}{2m}\right)^{\underline{2}} = \left(\frac{x^{\underline{2}} + m^2 + m}{2m}\right)^{\underline{2}},$$

where x is an integer such that $\dfrac{x^{\underline{2}}}{m}$ is odd.

Proof. This theorem comes directly out of the construction of the sets in the previous proof. □

Note that while equation (4) is similar to the equation $x^2 + y^2 = z^2$ from which the Pythagorean triples are derived, the equation for the Pythagorean triples is homogenous and birationally equivalent to the real line, which allows for a straight-forward parametrization of the set of integral solutions. As our equation is non-homogeneous, we do not have such a parametrization.

4 Factorial Cubes

The existence of numerous solutions to equation (1) for $n = 3$ is easily confirmed through a computer-assisted search. To investigate the cardinality of the solution set, we once again use the parameter $m = z - y$ to rewrite the equation as $x^{\underline{3}} + y^{\underline{3}} = (y + m)^{\underline{3}}$. From this we obtain the following theorem.

Theorem 4.1. *For all $m \in \mathcal{Z}$ there exist some $x, y, z \in \mathcal{Z}$ with $z - y = m$ such that $x^{\underline{3}} + y^{\underline{3}} = z^{\underline{3}}$.*

Proof. Given m, let $x = 3m^3 - 6m^2 + m + 2$, and $y = m(3m^3 - 9m^2 + 6m + 1)$. It can be shown that

$$x^{\underline{3}} = m^{\underline{2}}(3m^2 - 6m + 1)(3m^2 - 3m - 2)(3m^3 - 6m^2 + m + 1)$$

and

$$y^{\underline{3}} = m^{\underline{3}}(3m^{\underline{3}} + 1)(3m^3 - 6m^2 + 1)(3m^3 - 3m^2 + 1).$$

From this

$$x^{\underline{3}} + y^{\underline{3}} = m^{\underline{2}}(3m^{\underline{3}} + 2)(m(3m^{\underline{3}} + 2) - 1)(3m^3 - 6m^2 + 2).$$

Now $y + m = m(3m^3 - 9m^2 + 6m + 2)$ and it can be shown that

$$(y + m)^{\underline{3}} = m^{\underline{2}}(3m^{\underline{3}} + 2)(m(3m^{\underline{3}} + 2) - 1)(3m^3 - 6m^2 + 2).$$

Thus we have that $x^{\underline{3}} + y^{\underline{3}} = (y + m)^{\underline{3}}$.

□

Note that in the above construction $y > x$ and x is increasing for all $m \geq 2$. Therefore we see this construction gives distinct integral solutions.

With the existence of solutions for all m shown, we now consider the cardinality of the solution set for a given m.

Expanding and simplifying the equation $x^{\underline{3}} + y^{\underline{3}} = (y + m)^{\underline{3}}$ gives us the elliptic curve

$$x^3 - 3x^2 + 2x - 3my^2 + (6m - 3m^2)y - m^{\underline{3}} = 0,$$

where m is a fixed parameter. Note that $m = 0$ gives us only trivial solutions noted in Section 2.

With this in mind we now consider Siegel's Theorem on integral points on elliptic curves, stated below as in [4, p. 146]. It should be noted that the theorem is stated in the context of the projective real plane.

Theorem 4.2 (Siegel)**.** *Let C be a non-singular cubic curve given by an equation $F(x, y) = 0$ with integer coefficients. Then C has only finitely many points with integer coordinates.*

Now, we will show in the proof of the following theorem that every non-zero m the curve is non-singular, thus m has a finite number of corresponding non-trivial solutions.

Theorem 4.3. *For any non-zero integer m, there exists a finite non-zero number of pairs, $(x, y) \in \mathcal{Z}^2$ such that $x^{\underline{3}} + y^{\underline{3}} = (y + m)^{\underline{3}}$.*

Proof. By the previous theorem we know there exists at least one solution for all m.

Now, by setting $x = X/Z$ and $y = Y/Z$, and multiplying through by Z^3 we have the curve in homogeneous coordinates.

$$F(X,Y,Z) = X^3 - 3X^2Z + 2XZ^2 - 3mY^2Z + (6m - 3m^2)YZ^2 - m^{\underline{3}}Z^3$$

Calculating the partial derivatives, we get

$$\begin{aligned} \frac{\partial F}{\partial X} =& 3X^2 - 6XZ + 2Z^2 \\ \frac{\partial F}{\partial Y} =& (6m - 3m^2)Z^2 - 6mYZ \\ \frac{\partial F}{\partial Z} =& 2(2X + (m - 3m^2)Y)Z - 3(X^2 + mY^2 + m^{\underline{3}}Z^2). \end{aligned}$$

If $Z = 0$, then the gradient is $(3X^2, 0, 3(X^2 + mY^2))$. As $m \neq 0$, the gradient is 0 if and only if $X = 0$ and $Y = 0$. As $(0, 0, 0)$ does not exist in the projective space, we have no singular points.

If $Z \neq 0$, we can let $Z = 1$, and thus $\frac{\partial F}{\partial X} = 0$ if and only if $X = \frac{1}{3}(3 \pm \sqrt{3})$, and $\frac{\partial F}{\partial Y} = 0$ if and only if $Y = (1 - \frac{m}{2})$. It can be shown that this point is not on the curve for any $m \in \mathcal{Z}$.

Thus, applying Siegel's Theorem we have that for any given m there exists a finite number of integer solutions to the equation $x^{\underline{3}} + y^{\underline{3}} = (y + m)^{\underline{3}}$. □

5 Higher Factorial Powers

Besides the trivial and simple solutions provided in Section 2, individual solutions to the equation for $n \geq 4$ are not as easy to find as they were in the cases of $n = 2, 3$. However, we have the following theorem.

Theorem 5.1. *For any $n \in \mathcal{Z}$ there exists an $N > n$ such that there exists a non-trivial solution to the equation $x^{\underline{N}} + y^{\underline{N}} = z^{\underline{N}}$.*

Proof. There exists a family of solutions to equation (1) for $n = 2$ of the form

$$x^{\underline{2}} + x^{\underline{2}} = z^{\underline{2}}$$

which can be obtained from the following formulas, which were derived using the work of Hong, Jeong, and Kwon [6] on the integral points on hyperbolas:

$$x_k = \frac{1}{2}\left(\frac{(1+\sqrt{2})^{2k+1} - (1-\sqrt{2})^{2k+1}}{\sqrt{8}} + 1\right)$$

$$z_k = \frac{1}{2}\left(\frac{(1-\sqrt{2})^{2k+1}) + (1+\sqrt{2})^{2k+1}}{2} + 1\right).$$

Given $2x^{\underline{2}} = z^{\underline{2}}$ it is easy to see that

$$2(z-2)^{\underline{z-x}} = z^{\underline{z-x}}.$$

The formula for the difference $z_k - x_k = m_k$ is given by

$$m_k = \frac{((3+2\sqrt{2})^k - (3-2\sqrt{2})^k)}{4\sqrt{2}}.$$

It can be shown that this function takes on integral values for all $k \in \mathcal{Z}$ and $m_k > k$ for all $k > 1$. Thus, given $n > 1$, we have the solution $2(z_n - 2)^{\underline{N}} = z_n^{\underline{N}}$, where $N = m_n > n$. □

The first few examples of this family of solutions are $19^{\underline{6}} + 19^{\underline{6}} = 21^{\underline{6}}$, $118^{\underline{35}} + 118^{\underline{35}} = 120^{\underline{35}}$, and $695^{\underline{204}} + 695^{\underline{204}} = 697^{\underline{204}}$.

6 Conclusions

We have developed a method to describe all solutions equation (1) for the case of $n = 2$, as well as an infinite family of solutions for the case of $n = 3$ and shown that there exists no maximal n for which non-trivial solutions exist.

In addition to these previously discussed solutions a computer aided search found only two other solutions for $n \leq 20$ and $x, y < 44000$. For the case of $n = 4$ it was found that $132^{\underline{4}} + 190^{\underline{4}} = 200^{\underline{4}}$ and for the case of $n = 6$ it was found that $14^{\underline{6}} + 15^{\underline{6}} = 16^{\underline{6}}$.

We are left with the following questions.

Question 6.1. Is 3 the greatest value of n for which an infinite family of solutions exist?

Question 6.2. Does there exist n such that no non-trivial solutions exist?

References

[1] A. Wiles, "Modular elliptic curves and Fermat's Last Theorem," *Annals of Mathematics*, V. 141, no. 3 (1995), pp. 443-551.

[2] Lenstra, Jr. H. W., "On the inverse Fermat equation", *Discrete Mathematics*, V. 106-107 (1992), pp. 329-331.

[3] Bennett, C. D., Glass, A. M.W., and Székely, G. J., "Fermat's last theorem for rational exponents," *The American Mathematical Monthly*, V. 111, no. 4 (2004), pp. 322-329.

[4] J. H. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.

[5] R. Graham, D. Knuth, O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*

[6] Hong, J., Jeong, K., and Kwon, J., "Integral points on hyperbolas," *Journal of Korean Mathematical Society*, V. 34, no. 1 (1997), pp. 149-157.