Hang Lung Mathematics Awards
Vol. 5 (2012)

Hang Lung Mathematics Awards 2012

Honorable Mention

Manipulating the Fermat's Equation

Team members:	Wing Man Chik, Ka Kit Ku, Ming Hong Lui, Long Hin Sin
Teacher:	Mr. Yan Ching Chan
School:	Po Leung Kuk Centenary Li Shiu Chung Memorial College

Hang Lung Mathematics Awards
Vol. 5 (2012), pp. 259–274

MANIPULATING THE FERMAT'S EQUATION

TEAM MEMBERS
Wing Man Chik, Ka Kit Ku,
Ming Hong Lui, Long Hin Sin

TEACHER
Mr. Yan Ching Chan

SCHOOL
Po Leung Kuk Centenary Li Shiu Chung Memorial College

Abstract. In our report, we will manipulate the Fermat's Equation by allowing one of the exponents to be arbitrary. It turns out that if a prime base is restricted, there are either no solutions or a unique primitive solution, depending on the residue class that the prime belonging to modulo 4.

1. Motivation

Our problem is motivated from the celebrated Fermat's Last Theorem. Solving the equation $x^k + y^k = z^n$ is definitely a great challenge. However, if we restrict z to be a prime number, then we may explicitly write down all the solutions by using no more than Basic Valuation Theory and Number Theory. In our report, we prove that the only solutions to $x^k + y^k = p^n$ are that $p = 2, 3$ or other primes $p \equiv 1 \pmod 4$.

In this chapter, we will state the theorem we are investigating.

1.1. The Case $p = 3$

Theorem 1. *For all positive integers $n > 1$, if there exists relatively prime positive integers x, y, where $x \geq y$ and an integer $k > 1$ such that*

$$x^k + y^k = 3^n,$$

then $(x, y, k, n) = (2, 1, 3, 2)$.

Proof. Either both x, y are multiples of 3, which is rejected or $3 \nmid xy$. Therefore if k is even, x^k and y^k are congruent to 1 mod 3 and their sum is congruent to 2 mod 3,

which is not a power of 3. If k is odd and $k > 1$, then $3^n = (x+y)(x^{k-1} - x^{k-2}y + \cdots + y^{k-1})$. Thus $x + y = 3^m$ for some integers $m \geq 1$. We will show that $n \geq 2m$. Moreover, since $y \equiv -x \pmod 3$, $x^{k-1} - x^{k-2}y + \cdots + y^{k-1} \equiv x^{k-1} + \cdots + x^{k-1} \equiv kx^{k-1} \pmod 3$, which yields $3 \mid k$.

By putting $x_1 = x^{k/3}$ and $y_1 = y^{k/3}$, we may assume that $k = 3$. Then $x^3 + y^3 = 3^n$ and $x + y = 3^m$. To prove $n \geq 2m$, it suffices to prove that $x^3 + y^3 \geq (x+y)^2$ or $x^2 - xy + y^2 \geq x + y$. Since $x \geq y + 1$, $x^2 - x = x(x-1) \geq xy$, we have $(x^2 - xy - x) + (y^2 - y) \geq y(y-1) \geq 0$ and $n \geq 2m$ is proved.

From the identity $(x+y)^3 - (x^3 + y^3) = 3xy(x+y)$, it follows that

$$3^{2m-1} - 3^{n-m-1} = xy$$

But $2m - 1 \geq 1$ and $n - m - 1 \geq n - 2m \geq 0$. If strict inequality holds in either place in the last inequality, then 3^{n-m-1} contains factor 3 and $3^{2m-1} - 3^{n-m-1}$ is divisible by 3, but xy is not. Contradiction arises.

Therefore, $m = 1$ and $n = 2$. Substituting into the equation, $(x, y, n, k) = (2, 1, 2, 3)$. □

After finishing the case $p = 3$, we want to further investigate the situation when p is extended to all primes. So, let's clearly state the statement of our thought.

Theorem 2. *For an odd positive integer k, any positive integers x, y, n and a prime p, where $x \geq y$ and $k, n > 1$ such that*

$$x^k + y^k = p^n,$$

the only solutions are $(x, y, p, k, n) = (2^m, 2^m, 2, k, mk + 1)$,$(2(3^t), 3^t, 3, 3, 2 + 3t)$, where m is a positive integer and t is a non-negative integer.

Theorem 3. *For an even positive integer k, any positive integers x, y, n and a prime p, where $x \geq y$ and $k, n > 1$ such that*

$$x^k + y^k = p^n,$$

it only has solutions when $p = 2$ or $p \equiv 1 \pmod 4$. In particular, if $p = 2$, $(x, y, k, n) = (2^m, 2^m, k, mk + 1)$, where m is a positive integer. If $p \equiv 1 \pmod 4$ and $(x, y) = 1$, then $x = |a_n|, y = |b_n|$ with a_n, b_n satisfying $a_n + b_n i = \pi^n$, where π is a Gaussian prime dividing p and $k = 2$.

Our final goal is to verify these two theorems.

2. Essential Tools

In this chapter, we will briefly go over all the necessary knowledge and theorems we need in solving the generalized equations. This involves the idea of quadratic reciprocity and the p-adic valuation.

2.1. Quadratic Residue

Definition 4. *For all integers a such that $(a, m) = 1$, a is called a* ***quadratic residue*** *modulo m if $x^2 \equiv a \pmod{m}$ has a solution. Otherwise, it is called a* ***quadratic nonresidue*** *modulo m.*

Example 5. *2 is a quadratic residue mod 7 as $3^2 \equiv 2 \pmod{7}$, whereas 2 is a nonresidue mod 5.*

Definition 6 (Legengre's Symbol)**.** *If p is an odd prime, then the Legengre Symbol $\left(\frac{a}{p}\right)$ is defined as*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue of } p \\ -1, & \text{if } a \text{ is not a quadratic residue of } p \\ 0, & \text{if } p \mid a \end{cases}$$

Example 7. *From* ***Example 5****, $\left(\frac{2}{7}\right) = 1$ and $\left(\frac{2}{5}\right) = -1$.*

Here, we quote some of the propositions about Legengre's Symbol. [See reviewer's comment (3)]

Proposition 8. *If p is a prime, then*

1) (Euler's criterion) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

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

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

4) If $(a, p) = 1$, then $\left(\frac{a^2}{p}\right) = 1$.

Proof. Refer to [1] Niven, Zuckerman. □

Theorem 9. *If $p \equiv 3 \pmod{4}$ and $p \mid a^2 + b^2$, then $p \mid a$ and $p \mid b$.*

Proof. $p \mid a^2 + b^2$ implies $a^2 + b^2 \equiv 0 \pmod{p}$. We have $a^2 \equiv -b^2 \pmod{p}$ after rearranging terms. We know that $\left(\frac{-b^2}{p}\right) = 1$ or 0 as a has a solution. If $\left(\frac{-b^2}{p}\right) = 1$, by **Proposition 8**, $\left(\frac{-1}{p}\right)\left(\frac{b^2}{p}\right) = 1$. We find that $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ by **Euler's criterion**. As $p \equiv 3 \pmod{4}$, $(p-1)/2$ is odd and $\left(\frac{-1}{p}\right) = -1$. This leads to a contradiction so $\left(\frac{-b^2}{p}\right) = 0$ and $p \mid b$.
As $p \mid a^2 + b^2$ with $p \mid b, p \mid a^2$ and so $p \mid a$. We're done. □

2.2. p-adic Valuation

Definition 10. *Let p be a prime number. For all positive integers n, there exists a unique l such that $n = p^l m$, where l, m are integers and $p \nmid m$. Here we define $\nu_p(n) = l$.*

The p-adic map is defined as $n \to \nu_p(n)$ and it plays a very important role in solving many number theory problems. Note that we define $\nu_p(0) = \infty$.

There are some properties about the p-adic function, which are essential to solve number theory problems.

Proposition 11. *For non-negative integers a, b and p is a prime, [See reviewer's comment (4)]*

1) $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.
2) $\nu_p((a,b)) = min(\nu_p(a), \nu_p(b))$ and $\nu_p([a,b]) = max(\nu_p(a), \nu_p(b))$.
3) $\nu_p(a+b) \geq min(\nu_p(a), \nu_p(b))$, and equality holds if and only if $\nu_p(a) \neq \nu_p(b)$.

Remark 12. *(a,b) is the g.c.d. of a and b and $[a,b]$ is the l.c.m. of a and b.*

The first two are trivial results so we only show the third proposition.

Proof. Let $a = p^m k$ and $b = p^n l$, where $p \nmid kl$. When $m = n$, it becomes

$$a + b = p^m k + p^m l = p^m (k + l)$$

p may be or may not be a factor of $k + l$, making that

$$\nu_p(a+b) = \nu_p(p^m(k+l)) \geq m = min(\nu_p(a), \nu_p(b))$$

We now prove the necessity part. When $m < n$ (equivalent to $\nu_p(a) < \nu_p(b)$),

$$a + b = p^m k + p^n l = p^m (k + p^{n-m} l)$$

As $p \nmid k + p^{n-m} l$, we have

$$\nu_p(a+b) = \nu_p(p^m(k+p^{n-m}l)) = m = min(\nu_p(a), \nu_p(b))$$

For the suffiency part, we have

$$\nu_p(a+b) = \nu_p(p^m k + p^n l) = \nu_p(p^m(k+p^{n-m}l)) = m + \nu_p(k+p^{n-m}l)$$

We know that $min(\nu_p(a), \nu_p(b)) = m$ when $m \leq n$, but equality is impossible as p can be a factor of $k + l$, making that $\nu_p(a+b) \neq min(\nu_p(a), \nu_p(b))$. Hence $m < n$ and $\nu_p(a) \neq \nu_p(b)$. We're done. □

Here, we have one more definition.

Definition 13. *For all non-negative integers a, b and $b \neq 0, \nu_p(\frac{a}{b}) = \nu_p(a) - \nu_p(b)$.*

As rational numbers can be written as $\frac{a}{b}$ in many different ways, if $\frac{a}{b} = \frac{c}{d}$ for some $c, d \in \mathbb{Z}$, then $\nu_p(a) - \nu_p(b) = \nu_p(c) - \nu_p(d)$. Since $ad = bc$, by **Proposition 11**.1, we have

$$\nu_p(a) + \nu_p(d) = \nu_p(ad) = \nu_p(bc) = \nu_p(b) + \nu_p(c)$$

Each rational number will output a unique value. As a result, we can extend the function to $\nu_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$.

Theorem 14 (Lifting Exponent Lemma)**.** *Let p be an odd prime and a, b are integers such that $p \nmid ab$ and $p \mid a - b$. Then for all $n \geq 1$, we have*

$$\nu_p(a^n - b^n) = \nu_p(a - b) + \nu_p(n)$$

Proof. Firstly, when $\nu_p(n) = 0$, it means $p \nmid n$. We want to show that $\nu_p(a^n - b^n) = \nu_p(a - b)$. Note that $a \equiv b \pmod{p}$. We find out that $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$. Moreover,

$$\begin{aligned}(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) &\equiv a^{n-1} + a^{n-1} + \cdots a^{n-1} \\ &= na^{n-1} \pmod{p}\end{aligned}$$

a, n are not multiples of p, making that $\nu_p(a^n - b^n) = \nu_p(a - b)$, as desired.

Secondly, we prove it for $n = p$. This time, we need to prove that p divides $a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}$ exactly once. Let $b = a + pk$ for some integers k. By **Binomial Theorem**, we know that $b^i \equiv a^i + ipka^{i-1} \pmod{p^2}$, so

$$\frac{a^p - b^p}{a - b} = \sum_{i=0}^{p-1} a^{p-1-i}b^i \equiv \sum_{i=0}^{p-1}(a^{p-1} + ipka^{p-2}) = pa^{p-1} + p^2\frac{p-1}{2}ka^{p-2} \equiv pa^{p-1} \pmod{p^2}$$

This shows that p divides $a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}$ exactly once.

Finally, to prove the general case $\nu_p(n) \geq 1$, we use induction.
Suppose the theorem holds when $\nu_p(n) = l$.
Then for $\nu_p(n) = l+1, \nu_p(n/p) = l$. Then by the theorem, we have $\nu_p(a^{n/p} - b^{n/p}) = \nu_p(n/p) + \nu_p(a - b)$. From the second case, together we have

$$\begin{aligned}\nu_p(a^n - b^n) = \nu_p(a^{(n/p)p} - b^{(n/p)p}) &= \nu_p(p) + \nu_p(a^{(n/p)} - b^{(n/p)}) \\ &= 1 + \nu_p(n/p) + \nu_p(a - b) \\ &= l + 1 + \nu_p(a - b) \\ &= \nu_p(a - b) + \nu_p(n)\end{aligned}$$

By induction, we know the theorem holds. □

Remark 15. *Note that this theorem in **NOT** applicable to $p = 2$ as from the second case of the proof, $\frac{p-1}{2}$ is not an integer. Therefore we have a spacial theorem for the case $p = 2$.*

Theorem 16 (Lifting Exponent Lemma for $p = 2$)**.** *Let x, y be odd integers and n be an even positive integer. Then*

$$\nu_2(x^n - y^n) = \nu_2(\frac{x^2 - y^2}{2}) + \nu_2(n)$$

Proof. Let $n = 2^k a$ for some odd integers a. Then

$$x^n - y^n = (x^a - y^a)(x^a + y^a)(x^{2a} + y^{2a}) \cdots (x^{2^{k-1}a} + y^{2^{k-1}a})$$

We can observe that if u, v are odd integers, then $u^2 + v^2 \equiv 2 \pmod 4$. Therefore,

$$\nu_2(x^n - y^n) = \nu_2(x^{2a} - y^{2a}) + k - 1$$

So what is the relation between $\nu_2(x^{2a} - y^{2a})$ and $\nu_2(x^2 - y^2)$?

Actually, we found that

$$\frac{x^{2a} - y^{2a}}{x^2 - y^2} = \frac{(x^a + y^a)(x^a - y^a)}{(x + y)(x - y)} = \sum_{i=0}^{a-1} (-1)^i x^{a-1-i} y^i \sum_{i=0}^{a-1} x^{a-1-i} y^i$$

All the terms are odd so we need to determine the number of terms.
Both summation systems have a terms, which are odd, so $\frac{(x^{2a} - y^{2a})}{x^2 - y^2}$ is actually odd.

$$\nu_2(\frac{x^{2a} - y^{2a}}{x^2 - y^2}) = 0$$

and

$$\nu_2(x^{2a} - y^{2a}) = \nu_2(x^2 - y^2)$$

Finally,

$$\begin{aligned} \nu_2(x^n - y^n) &= \nu_2(x^2 - y^2) + k - 1 \\ &= \nu_2(\frac{x^2 - y^2}{2}) + \nu_2(n) \end{aligned}$$

and we're done. □

2.3. Gaussian Integers

Definition 17 (Gaussian Integers)**.** *The set of Gaussian Integers is defined to be $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.*

Definition 18 (Unit)**.** *An element $\alpha = a + bi \in \mathbb{Z}[i]$ is a unit if there is another element $\beta = c + di \in \mathbb{Z}[i]$ such that $\alpha\beta = 1$.*

The units of Gaussian Integers are $\{1, -1, i, -i\}$.
So what is a prime under $\mathbb{Z}[i]$? We have the following definition.

Definition 19 (Prime)**.** *For an element $\alpha \in \mathbb{Z}[i]$, we call it a prime under $\mathbb{Z}[i]$ if it cannot be written as $\alpha = \beta\gamma$, where $\beta, \gamma \in \mathbb{Z}[i]$ and they are not units. If α is a prime and it is also a prime in $\mathbb{Z}$, we call it a **rational prime**.*

Definition 20 (Norm)**.** *The norm of $\alpha = a + bi$ is defined as $N(\alpha) = (a + bi)(a - bi) = \alpha\bar{\alpha} = a^2 + b^2$. The norm is multiplicative, i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$.*

The arithmetic in $\mathbb{Z}$ is similar to that in $\mathbb{Z}[i]$, so all the theorem about division can also be applied in $\mathbb{Z}[i]$. Here, we quote one that is useful to us.

Theorem 21 (Unique Factorization Theorem)**.** *Every non-zero, non-unit $\alpha \in \mathbb{Z}[i]$ can be written as a unique product of primes up to order and multiplication of units.*

With all these definitions, we can deduce a very essential theorem which will be at utmost importance for us to obtain the solutions for the equation.

Theorem 22. *There are infinite number of primes p that can be written into sum of two squares if $p \equiv 1 \pmod 4$. [See reviewer's comment (5)]*

Proof. Refer to [2] Niven, Zuckerman, Montgomery. □

3. Success of Generalization

After going through all the necessary tools we will use, let's see if these will help us in attempting the general case.

3.1. The Case $p = 3$ by p-adic Valuation

Let's recall what the theorem is.

Theorem 23. *For all positive integers n, if there exist relatively prime positive integers x, y, where $x \geq y$ and an integer $k > 1$ such that*

$$x^k + y^k = 3^n,$$

then $(x, y, k, n) = (2, 1, 3, 2)$.

Proof. We can observe that $3 \mid x^k + y^k$. If k is even, by **Theorem 9**, $3 \mid x$ and $3 \mid y$ and contradict to the requirement of $(x, y) = 1$.

When k is odd, $x^k + y^k = (x + y)(x^{k-1} - \cdots + y^{k-1}) = 3^n$, meaning $x + y = 3^m$ for some $m \geq 1$, or $x + y = 1$, which is absurd. [See reviewer's comment (6)] By the **Lifting Exponent Lemma**, we have

$$\nu_3(x^k + y^k) = \nu_3(x + y) + \nu_3(k)$$

Rearranging terms we have $m = n - \nu_3(k)$.

Case 1: $m \geq 2$. We observe that $3^a \geq a+2$ for $a \geq 1$ since LHS grows exponentially faster than RHS. Putting $a = \nu_3(k)$, we have $\nu_3(k) \leq 3^{\nu_3(k)} - 2 \leq k - 2$.

Since $x + y = 3^m \geq 9$, we have $M := max(x, y) > 3$. Moreover,

$$M \geq \frac{x+y}{2} = \frac{3^m}{2}$$

Hence,

$$\begin{aligned} x^k + y^k \geq M^k = M \cdot M^{k-1} &> \frac{3^m}{2} \cdot 3^{k-1} \\ &> \frac{3^m}{3} \cdot 3^{k-1} \\ &= 3^{m+k-2} \\ &\geq 3^{m+\nu_3(k)} \\ &= 3^n \end{aligned}$$

It is a contradiction.

Case 2: $m = 1$. Then $x + y = 3$ and $(x, y) = (1, 2)$ or $(2, 1)$. Rearranging the equation yields $3^n - 2^k = 1$. By **Catalan's Theorem**[1], we have $n = 2$ and $k = 3$. □

This method saves time to eliminate all possible values of k other than 3, unlike the previous proof. It gives us a hope to tackle the generalized form by using p-adic valuation.

3.2. The Case $p = 2$

We first look into the case where $p = 2$.
As $x, y > 0, x^k + y^k \geq 1 + 1 = 2$, which means $n \geq 1$. When $n \geq 1$, 2^n must be even so x and y must be both odd or both even.

Case 1: x, y are odd.

Case 1.1: k is even.
Rearranging the terms, we have $x^k - y^k = 2^n - 2y^k$. Therefore $\nu_2(x^k - y^k) = \nu_2(2^n - 2y^k)$.

By **Theorem 16**, $\nu_2(\frac{x^2 - y^2}{2}) + \nu_2(k) = \nu_2(2(2^{n-1} - y^k)$.
Noticing $2^{n-1} - y^k$ is odd, we have

$$\begin{aligned} \nu_2(x^2 - y^2) - 1 + \nu_2(k) &= 1 \\ \nu_2(k) &= 2 - \nu_2(x^2 - y^2) \\ &= 2 - \nu_2(x + y) - \nu_2(x - y) \end{aligned}$$

If $x = y$, it will become

$$x^k + y^k = 2x^k = 2^n$$

[1]From [3] Mihăilescu

It has no solutions as LHS has odd factors where RHS is a perfect power of 2. [See reviewer's comment (7)]

Now suppose $x \neq y$. Since x, y are both odd, $x + y$ and $x - y$ are even. It comes up with

$$\nu_2(x+y), \nu_2(x-y) \geq 1$$

and we have

$$\nu_2(k) \leq 0$$

which is absurd.

Case 1.2: k is odd.
We can factorize the equation.

$$x^k + y^k = (x+y)(x^{k-1} - x^{k-2}y + \cdots - xy^{k-2} + y^{k-1}) = 2^n$$

Recall x and y are odd, $y \equiv -x \pmod 2$, so

$$\begin{aligned} x^{k-1} - x^{k-2}y + \cdots - xy^{k-2} + y^{k-1} &\equiv x^{k-1} + x^{k-1} + \cdots + x^{k-1} \\ &= kx^{k-1} \pmod 2. \end{aligned}$$

Thus $2 \nmid x^{k-1} - x^{k-2}y + \cdots - xy^{k-2} + y^{k-1}$.
Also, if $x \geq y > 1$, then

$$\begin{aligned} & x^{k-1} - x^{k-2}y + \cdots - xy^{k-2} + y^{k-1} \\ =& x^{k-2}(x-y) + x^{k-4}(x-y) + \cdots + xy^{k-3}(x-y) + y^{k-1} \\ =& (x-y)(x^{k-2} + x^{k-4} + \cdots + xy^{k-3}) + y^{k-1} \\ >& 1 \end{aligned}$$

LHS consists of factors other than 2, but RHS is a perfect power of 2, which is a contradiction.

Case 2: x, y are even
Let $x = 2^\alpha a$ and $y = 2^\beta b$, where a, b are odd positive integers and $\alpha, \beta > 0$. Then

$$x^k + y^k = (2^\alpha a)^k + (2^\beta b)^k = 2^n$$

If $\alpha < \beta$, the equation becomes

$$a^k + 2^{(\beta-\alpha)k} b^k = 2^{n-\alpha k}$$

We have LHS is odd but RHS is even. So it has no solutions.
Similarly, it has no solutions when $\alpha > \beta$. When $\alpha = \beta$, the equation becomes

$$a^k + b^k = 2^{n-\alpha k}$$

One trivial solution is $a = b = 1$ and $n = \alpha k + 1$. In fact, by putting $a = b = 2^m$, the general solution can be derived in the form of $(x, y, k, n) = (2^m, 2^m, k, mk + 1)$, where m is a positive integer. Note that the value of k can be arbitrary.

3.3. The Case for All Odd Primes

Then we consider the case for all odd primes, but before proceeding, we hope to divide k into two cases.

3.3.1. When k is odd

After factorization, we have

$$x^k + y^k = (x+y)(x^{k-1} - x^{k-2}y + \ldots - xy^{k-2} + y^{k-1}) = p^n$$

either p is a factor of $x+y$, or $x+y=1$. The latter case is impossible so p must divide $x+y$. Hence let $x+y=p^m$.
Therefore, we may apply the **Lifting Exponent Lemma**.

$$\nu_p(x^k + y^k) = \nu_p(x+y) + \nu_p(k) = n$$

So we have $m = n - \nu_p(k)$.

Case 1: $m \geq 2$.
We can see that $p^a \geq a+2$ for $p \geq 3$ and $a \geq 1$ as LHS grows exponentially faster that RHS. Substituting $a = \nu_p(k)$, we have $\nu_p(k) \leq p^{\nu_p(k)} - 2 \leq k-2$.

As $x+y = p^m \geq p^2$, let $M : max(x,y) > p$. Then we have

$$M \geq \frac{x+y}{2} = \frac{p^m}{2}$$

Hence,

$$\begin{aligned} x^k + y^k \geq M^k = M \cdot M^{k-1} &> \frac{p^m}{2} \cdot p^{k-1} \\ &> \frac{p^m}{p} \cdot p^{k-1} \\ &= p^{m+k-2} \\ &\geq p^{m+\nu_p(k)} \\ &= p^n \end{aligned}$$

It is a contradiction.

Case 2: $m = 1$. In this case, we have 2 equations.
$\begin{cases} x^k + y^k = p^n \\ x + y = p \end{cases}$
Moreover, from the **Lifting Exponent Lemma**, we know that $\nu_p(k) = n-1$. Therefore, $x^k + y^k = x^{p^{n-1}l} + y^{p^{n-1}l} = p^n$, where $p \nmid l$.
As $x^{p^{n-1}} + y^{p^{n-1}} \leq x^{p^{n-1}l} + y^{p^{n-1}l}$ for $1 \leq l$, we shall have to prove that either $x^{p^{n-1}}$ or $y^{p^{n-1}}$ is greater than p^n.

Case 2.1: $n = 2$. Then $x^{p^l} + y^{p^l} = p^2$.
We will prove the following inequality: $x^p > p^2$ for all $p > 4$ and $x > 1$.
Since $x^p \geq 2^p$, it suffices to prove $2^p > p^2$.

For $p = 5, 2^5 = 32 > 5^2$.
Assume the result holds when $p = k$, i.e. $2^k > k^2$.
When $p = k + 1, (k + 1)^2 = k^2 + 2k + 1$. As

$$k^2 - 2k - 1 = k^2 - 2k + 1 - 2 = (k - 1)^2 - 2 > 0 \Rightarrow k^2 > 2k + 1$$

for $k \geq 5$, we have

$$(k + 1)^2 = k^2 + 2k + 1 < 2k^2 < 2(2^k) = 2^{k+1}$$

By induction, we have $2^p > p^2$.

Since $x^{p^l} \geq x^p \geq 2^p > p^2$, we have $x^{p^l} + y^{p^l} \geq x^p + y^p > p^2$, and x, y, p, k have no integral solutions. It doesn't matter if the values of x and y are interchanged. Since $x + y = p$ with $p > 4$, either x or y must be greater than 2.

The case $p = 3$ is done in **Theorem 1** and $(x, y, k, p, n) = (1, 2, 3, 3, 2)$ or $(2, 1, 3, 3, 2)$. But to obtain a general solution, we can multiply both sides by 3^3 and have new sets of solutions.
So

$$(x, y, p, k, n) = (3^t, 2(3^t), 3, 3, 2 + 3t), (2(3^t), 3^t, 3, 3, 2 + 3t),$$

where t is a non-negative integer.

Case 2.2: $n > 2$. This time, we need to prove a stronger inequality: $x^{p^{n-1}} > p^n$ for $x > 1$ and $p > 2$. As $x^{p^{n-1}} \geq 2^{p^{n-1}}$, we'll check if $2^{p^{n-1}} > p^n$.
When $n = 3$, LHS=2^{p^2}. By **Binomial Theorem**, we have

$$\begin{aligned} 2^{p^2} = (1 + 1)^{p^2} &\geq \binom{p^2}{1} + \binom{p^2}{2} + \binom{p^2}{p^2 - 2} \\ &= p^4 \\ &> p^3 \end{aligned}$$

Suppose it is true for some $k \geq 3$. Then

$$2^{p^k} = (2^{p^{k-1}})^p > (p^k)^p > p(p^k) = p^{k+1}$$

We are done by induction.

As $x^{p^{n-1}l} \geq x^{p^{n-1}} \geq 2^{p^{n-1}} > p^n, x^{p^{n-1}l} + y^{p^{n-1}l} \geq x^{p^{n-1}} + y^{p^{n-1}} > p^n$, which means x, y, p, k have no integral solutions.

3.3.2. When k is even

Case 1: $p \equiv 3 \pmod 4$
Let $k = 2l$, where l is a positive integer. The equation becomes

$$x^k + y^k = x^{2l} + y^{2l} = (x^l)^2 + (y^l)^2 = p^n$$

If such solution exists, we have $p \mid ((x^l)^2 + (y^l)^2)$. By **Theorem 9**, we have p divides both x^l and y^l, implying $p \mid x$ and $p \mid y$.
Now let $x = ap^c, y = bp^d$, where $p \nmid a, b$.
The equation then becomes

$$(ap^c)^k + (bp^d)^k = p^n$$

Without loss of generality, assume $d \geq c$. Dividing both sides by p^{ck},

$$a^k + (bp^{d-c})^k = p^{n-ck}$$

We can see that $d = c$ is a must, or else $p \nmid$ LHS. Then the equation can be reduced to $a^k + b^k = p^{n-ck}$.
By **Theorem 9** again, we know that a, b have a solution only if $p \mid a$ and $p \mid b$, which is a contradiction here.
Therefore, there are no solutions for all $p \equiv 3 \pmod 4$ and $p > 3$.

Case 2: $p \equiv 1 \pmod 4$

Case 2.1: When $k \neq 2^m$, where m is a positive integers.
Let $k = 2^g h$, where g is a positive integer and $2 \nmid h$. The equation becomes

$$x^{2^g h} + y^{2^g h} = p^n$$

The equation is reduced to a new form where h becomes the corresponding k of the original equation.
We can observe that the new equation can fit into the case where k is odd.
$(x^{2^g}, y^{2^g}, p, h, n) = (2, 2^m, 2^m, k, mk + 1), (3, 3^m, 2(3^m), 3, 2 + 3m)$ and
$(3, 2(3^m), 3^m, 3, 2 + 3m)$.
There are no integral solutions for $(x^{2^g}, y^{2^g}) = (2^m, 2^m)$ or $(3^m, 2(3^m))$ or $(2(3^m), 3^m)$. Therefore the equation has no integral solutions when $k \neq 2^m$, where m is a positive integer.

Case 2.2: When $k = 2$.
Since $p \equiv 1 \pmod 4$, we can factorize $p = \pi\bar{\pi}$, where $\pi, \bar{\pi}$ are Gaussian integers. In LHS, $x^2 + y^2 = (x + yi)(x - yi)$. In general, we have

$$(x + yi)(x - yi) = \pi^n \bar{\pi}^n$$

Here, we can put $x + yi = \pi^n$ and $x - yi = \bar{\pi}^n$. Suppose $\pi = a + bi$, where a, b are integers. Then we can get $a_n + b_n i$ by expanding π^n. Similarly, $x - yi = \bar{\pi}^n = \overline{\pi^n} = a_n - b_n i$. Hence we can deduce $x = Re(\pi^n) = |a_n|$ and $y = Im(\pi^n) = |b_n|$.
The key to find a_n and b_n is to identify a, b from the beginning first. After that it is all left to find them by brute force.

Of course, you may not choose x, y in this way. Let $x + yi = \pi^{n-1}\bar{\pi}$ and $x - yi = \bar{\pi^{n-1}}$. Then

$$\pi^{n-1}\bar{\pi} = \pi^{n-2}\pi\bar{\pi} = p\pi^{n-2}$$

You will see that x, y both contain factor p after expanding $p\pi^{n-2}$. So we have

$$p^{\theta k}c^k + p^{\theta k}d^k = p^n,$$

for some c, d, θ. But dividing both sides by $p^{\theta k}$, then we will have

$$c^k + d^k = p^{n-\theta k}$$

Actually this is a set of solutions comes from the first method of choosing the factors.

Case 2.3: When $k = 2^m$, where $m \geq 1$.
This time we factorize the LHS in a different way.

$$x^{2^m} + y^{2^m} = x^{(2^{m-1})2} + y^{(2^{m-1})2} = p^n$$

The intermediate steps are the same but the only difference is to compare

$$x^{2^{m-1}} = Re(\pi^n) = |a_n|$$

and

$$y^{2^{m-1}} = Im(\pi^n) = |b_n|$$

To have x, y to be integers, a_n and b_n must be 2^{m-1}-th powers.

After investigation, we can conclude that there are solutions for the equation only when $p = 2, p = 3$ and $p \equiv 1 \pmod 4$. In particular, when $p = 2$, $(x, y, k, n) = (2^m, 2^m, k, mk + 1)$, where m is a positive integer.
When $p = 3$, $(x, y, k, n) = (2(3^t), 3^t, 3, 2 + 3t)$, where t is a non-negative integer.
When $p \equiv 1 \pmod 4$, if $(x, y) = 1$, then $(x, y, k, n) = (|\alpha|, |\beta|, 2, n)$, where α, β satisfy $\alpha + \beta i = \pi^n$, with π being a Gaussian prime dividing p.
If $(x, y) \neq 1$, then $(x, y) = (p^m\alpha, p^m\beta)$, where α, β satisfy $\alpha + \beta i = \pi^{n-m}$, with π being a Gaussian prime dividing p and $m < n$. Based on these results, the two theorems in Chapter 1 are proved.

4. Beyond

4.1. Obstacles for general case: Composite numbers z

After the generalization, we want to investigate further. We then modify our aspect. Instead of a prime number p, we want to find out what happens when a natural number z is replaced, i.e.

$$x^k + y^k = z^n$$

However, the proof of generalization does not work with composite z. Let's see which part fails.

4.1.1. Attempt by using the same approach

Suppose we divide k into two case: k is odd and k is even.

If k is odd, then we factorize $x^k + y^k = (x+y)(x^{k-1} - x^{k-2}y \cdots + y^{k-1}) = z^n$. Since z consists of primes, there will be many different combinations for the values in both terms in LHS. This means solving the equation $x^k + y^k = z^n$ by means of Elementary Number Theory will be abysmally hopeless. In particular, the case $n = k$ was solved by Prof. Andrew Wiles in 1995 using advanced theory of Elliptic Curve and Modular Form.

Yet, in here, we approach a further generalization in the following ways.

1. Fixing the index k.
2. Fixing the base value z.

4.1.2. The Case $z = 14$, $k = 3$

Let's see if we can solve this equation.

$$x^3 + y^3 = 14^n$$

Factorizing both sides yields

$$(x+y)(x^2 - xy + y^2) = 2^n 7^n$$

Supposes $x + y = 2^\alpha 7^\beta$ and $x^2 - xy + y^2 = 2^{n-\alpha}7^{n-\beta}$, where α, β are non-negative integers. From the first equation, we have $x = 2^\alpha 7^\beta - y$. Put this in the latter equation, we have [See reviewer's comment (8)]

$$x^2 - xy + y^2 = y^2 - y(2^\alpha 7^\beta - y) + (2^\alpha 7^\beta - y)^2 = 2^{n-\alpha}7^{n-\beta}$$

Rearranging yields $3y^2 - 3(2^\alpha 7^\beta)y + 2^{2\alpha}7^{2\beta} - 2^{n-\alpha}7^{n-\beta} = 0$. It becomes a quadratic equation in y. We then try to find the discriminant Δ.

$$\begin{aligned}\Delta &= 9(2^{2\alpha}7^{2\beta}) - 12(2^{2\alpha}7^{2\beta} - 2^{n-\alpha}7^{n-\beta}) \\ &= -3(2^\alpha 7^\beta)^2 + 12(2^{n-\alpha}7^{n-\beta})\end{aligned}$$

Substitution yields $\Delta = -3(x+y)^2 + 12(x^2 - xy + y^2) = [3(x-y)]^2$. We can see that the discriminant is a perfect square, which means that integer solutions exist. Using the quadratic formula, we have

$$\begin{aligned}y &= \frac{3(2^\alpha 7^\beta) \pm 3(x-y)}{6} \\ 6y &= 3(x+y) \pm 3(x-y)\end{aligned}$$

If $6y = 3(x+y) - 3(x-y)$, it yields $0 = 0$, which is useless for us. Therefore $6y = 3(x+y) + 3(x-y)$ is our only hope. Yet

$$\begin{aligned} 6y &= 3(x+y) + 3(x+y-2y) \\ 12y &= 2 \cdot 3(x+y) = 3(2^{\alpha+1}7^{\beta}) \\ y &= 2^{\alpha-1}7^{\beta} \end{aligned}$$

Substituting our result into $x+y = 2^{\alpha}7^{\beta}$, we have $x = y = 2^{\alpha-1}7^{\beta}$. However, if we put this equation back into the beginning, we have $2^{3\alpha-2}7^{3\beta} = 2^n 7^n$. Contradiction arises when we compare the indices taking modulo 3. Therefore there are no integral solutions for $x^3 + y^3 = 14^n$ for all x, y, n.

4.2. Summary

In Chapter 3 of this report, we successfully find out that for equation $x^k + y^k = p^n$, there exist solutions for primes 2, 3 and other primes $p \equiv 1 \pmod 4$.
Let's recall what the solutions are for $p = 2, 3$ (for the case $p \equiv 1 \pmod 4$, the existence is proved but the form of solutions cannot be explicitly written).
If $p = 2, (x, y, k, n) = (2^m, 2^m, k, mk+1)$, where m is a positive integer.
If $p = 3, (x, y, k, n) = (3^t, 2(3^t), 3, 2+3t), (2(3^t), 3^t, 3, 2+3t)$, where t is a non-negative integer. (If $x \geq y$, then the set of solutions $(3^t, 2(3^t), 3, 2+3t)$ is rejected)

Then in Chapter 4, we try to extend prime numbers p into all natural numbers z, i.e. $x^k + y^k = z^n$.
Our theorem is not applicable to composite numbers so we try to attack it case by case. The new equation is way far beyond the Fermat's equation. We are not able to solve it generally but to tackle it by fixing different indices k and the base value z.

REFERENCES

[1] Amir H. Pavardi, *Lifting Exponent Lemma*, http://s3.amazonaws.com/aops-cdn.artofproblemsolving.com/resources/articles/lifting-the-exponent.pdf

[2] Ivan Niven, Herbert S. Zuckerman and Hugh L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., Courier Companies. Inc., 1991.

[3] Kenneth Ireland, Michael Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 2010.

[4] Preda Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. **572** (2004), 167-195.

[5] Titu Andreescu, Dorin Andrica and Ion Cucurezeanu, *An Introduction to Diophantine Equations*, Birkhäuser Boston, 2010.

Reviewer's Comments

The presentation of the paper is good. The following is an incomplete list of corrections and stylistic suggestions.

1. The reviewer has comments on the wordings, which have been amended in this paper.
2. Punctuation marks are missing in most of the formulas in this paper.
3. "of the propositions" should be rewritten as "results".
4. "p is a prime" should be rewritten as "any prime".
5. "number of" should be deleted.
6. "meaning" should be rewritten as "implying".
7. "where" should be rewritten as "while".
8. "Put" should be rewritten as "Substituting".