

Integer Powers and Catalan- Mihăilescu Theorem

Kader S.

Abstract. Catalan- Mihăilescu Theorem states that the only case of difference between two consecutive powers equals 1 is $3^2 - 2^3$. This article provides some elementary analyses of integer powers, and proves in that light, Catalan- Mihăilescu Theorem.

Keywords: Integer, power, consecutive, co-prime

MSC (2020): 11D61, 11D41, 11D45

1. INTRODUCTION

Catalan's conjecture (or Mihăilescu's theorem) [1, 2] is a theorem in number theory that was conjectured by the Belgian mathematician Eugène Charles Catalan (1814-1894). The integers 2^3 and 3^2 are two powers of natural numbers whose values (8 and 9, respectively) are consecutive. The theorem states that this is the only case of two consecutive powers. That is to say, that the only solution in the natural numbers of the equation:

$$x^m - y^n = 1$$

for $m, n > 1$; $x, y > 0$ is $x = 3, m = 2, y = 2, n = 3$.

Catalan mentioned this conjecture as a problem in the section Théorèmes et problèmes on p. 520 of the first volume of the journal Nouvelles Annales de Mathématiques in 1842. [3] The conjecture was received by the editor of the Journal für die Reine und Angewandte Mathematik as a letter from Catalan, and published in the journal in 1844. [4] Catalan, at that time a teacher at l' Ecole Polytechnique de Paris, had won his reputation with a solution of a combinatorial problem. The term Catalan number, still in use, refers to that problem. As to the equation, Catalan wrote that he could not prove it completely so far. He never published any serious partial result about it either [1]. The only results of Catalan on this equation are simple observations in his Mélanges Mathématiques, XV, published much later in 1885. [5] Catalan's conjecture was proven by Preda Mihăilescu in April 2002. The proof was published in the Journal für die reine und angewandte Mathematik, 2004. It makes extensive use of the theory of cyclotomic fields and Galois modules [6]. This article provides some elementary analyses of integer powers, and proves in that light, Catalan- Mihăilescu Theorem.

2. INTEGER POWERS AND CATALAN- MIHĂILESCU THEOREM

Lemma 2.1. When x, y, m, n are positive integers, $x^m - y^n = 1$ then we have m, n co-primes.

Proof: Suppose, m, n are not co-primes. Let $m = r\mu, n = r\eta$ when μ, η are positive integers. Then

$$x^m - y^n = x^{r\mu} - y^{r\eta} = (x^\mu)^r - (y^\eta)^r = (x^\mu - y^\eta)((x^\mu)^{r-1} + \dots + (y^\eta)^{r-1}) \neq 1$$

Contradicts our equation. So, m, n are co-primes. □

Lemma 2.2. When x, y, m, n are positive integers, $x^m - y^n = 1$ then we have x, y co-primes.

Proof: Suppose, x, y are not co-primes. Let $x = r\alpha, y = r\beta$ when α, β are positive integers, $\alpha \neq \beta$. Then, if $n > m$ we have,

$$x^m - y^n = (r\alpha)^m - (r\beta)^n = r^m(\alpha^m - r^{n-m}\beta^n) \neq 1$$

if $m > n$ we have,

$$x^m - y^n = (r\alpha)^m - (r\beta)^n = r^n(r^{m-n}\alpha^m - \beta^n) \neq 1$$

if $m = n$ we have,

$$x^m - y^n = (r\alpha)^m - (r\beta)^n = (r\alpha)^m - (r\beta)^m = r^m(\alpha^m - \beta^m) \neq 1$$

All contradict our equation. So, x, y are co-primes. □

Lemma 2.3. When x, y, m, n are positive integers, $x^m - y^n = 1$ then x, y are not both odd.

Proof: Suppose, x, y are both odd. Then when k is an integer,

$$x^m - y^n = 2k \neq 1$$

Contradicts our equation. So, x, y are not both odd. \square

Lemma 2.4. $\forall u > 1, w \in \mathbb{N}, \exists z \in \mathbb{N}$, such that, $u^{2w} = (u+1)z + 1$ where $z = u(z_i u + 1) - 1$ when $0 = z_0 \leq z_i < z$, and z_i is immediate previous value of z . The formula defines parity of z which is odd when u even, even when u odd iterating over $z_0 = 0$.

Proof: We see,

| | | |
|---|---|--|
| $2^{2 \times 1} = 3 \times 1 + 1 = 4$ | $3^{2 \times 1} = 4 \times 2 + 1 = 9$ | $4^{2 \times 1} = 5 \times 3 + 1 = 16$ |
| $2^{2 \times 2} = 3 \times 5 + 1 = 16$ | $3^{2 \times 2} = 4 \times 20 + 1 = 81$ | $5^{2 \times 1} = 6 \times 4 + 1 = 25$ |
| $2^{2 \times 3} = 3 \times 21 + 1 = 64$ | $3^{2 \times 3} = 4 \times 182 + 1 = 729$ | $6^{2 \times 1} = 7 \times 5 + 1 = 36$ |

Here we see the pattern, $u^{2w} = (u+1)z + 1$.

By induction method, the next expression,

$$\begin{aligned} u^{2(w+1)} &= u^{2w+2} = u^2 \times u^{2w} = u^2((u+1)z + 1) \\ &= (u+1)zu^2 + u^2 = (u+1)zu^2 + u^2 - 1 + 1 = (u+1)(zu^2 + u - 1) + 1. \end{aligned}$$

Letting $w+1 = w_1$ and $zu^2 + u - 1 = u(zu + 1) - 1 = z_1$, the pattern of expression remains the same,

$$u^{2w_1} = (u+1)z_1 + 1$$

So by induction we prove, $\forall u, w \in \mathbb{N}, \exists z \in \mathbb{N}$, such that, $u^{2w} = (u+1)z + 1$, and also get the formula, $z = u(z_i u + 1) - 1$ when $0 = z_0 \leq z_i < z$, and z_i is immediate previous value of z . The formula defines parity of z which is odd when u even, even when u odd iterating over $z_0 = 0$. \square

Lemma 2.5. $\forall u > 1, w \in \mathbb{N}, \exists z \in \mathbb{N}$, such that, $u^{2w+1} = (u+1)z - 1$ where $z = u(z_i u - 1) + 1$ when $1 = z_0 \leq z_i < z$ ($z_0 = 0$ gives negative value), and z_i is immediate previous value of z . The formula defines parity of z which is odd when u even, odd when u odd iterating over $z_0 = 1$.

Proof: We see,

| | | |
|--|--|--|
| $2^{2 \times 1 + 1} = 3 \times 3 - 1 = 8$ | $3^{2 \times 1 + 1} = 4 \times 7 - 1 = 27$ | $4^{2 \times 1 + 1} = 5 \times 13 - 1 = 64$ |
| $2^{2 \times 2 + 1} = 3 \times 11 - 1 = 32$ | $3^{2 \times 2 + 1} = 4 \times 61 - 1 = 243$ | $5^{2 \times 1 + 1} = 6 \times 21 - 1 = 125$ |
| $2^{2 \times 3 + 1} = 3 \times 43 - 1 = 128$ | $3^{2 \times 3 + 1} = 4 \times 547 - 1 = 2187$ | $6^{2 \times 1 + 1} = 7 \times 31 - 1 = 216$ |

Here we see the pattern, $u^{2w+1} = (u+1)z - 1$.

By induction method, the next expression,

$$\begin{aligned} u^{2(w+1)+1} &= u^{2w+3} = u^2 \times u^{2w+1} = u^2((u+1)z - 1) \\ &= (u+1)zu^2 - u^2 = (u+1)zu^2 - u^2 + 1 - 1 = (u+1)(zu^2 - u + 1) - 1. \end{aligned}$$

Letting $w+1 = w_1$ and $zu^2 - u + 1 = u(zu - 1) + 1 = z_1$, the pattern of expression remains the same,

$$u^{2w_1+1} = (u+1)z_1 - 1$$

So by induction we prove, $\forall u, w \in \mathbb{N}, \exists z \in \mathbb{N}$, such that, $u^{2w+1} = (u+1)z - 1$, and also get the formula $z = u(z_i u - 1) + 1$ when $1 = z_0 \leq z_i < z$ ($z_0 = 0$ gives negative value), and z_i is immediate previous value of z . The formula defines parity of z which is odd when u even, odd when u odd iterating over $z_0 = 1$. \square

Corollary 2.6. When $u > 1, w, v \in \mathbb{N}$, either $w = v$ or $w \neq v$ we have,

(i)

$$u^{2w} \equiv 1 \pmod{u+1}$$

(ii)

$$u^{2v+1} \equiv -1 \pmod{u+1}$$

So,

$$u^{2w} \equiv u^{2v+1} + 2 \pmod{u+1}$$

$$u^{2w} + u^{2v+1} \equiv 0 \pmod{u+1}$$

Theorem 2.7 (Catalan- Mihăilescu Theorem). When x, y, m, n are positive integers, for

$$x^m - y^n = 1 \tag{2.1}$$

Only non-trivial solution is $(x, y, m, n) = (3, 2, 2, 3)$

Proof: (i)Relating lemma 2.4 to Catalan- Mihăilescu equation we have,

$$u^{2w} = (u+1)z + 1 = v^g + 1 \tag{2.2}$$

or subtracting 1 from (2.2) we have,

$$v^g = (u+1)z = u^{2w} - 1 = (u^w - 1)(u^w + 1)$$

We see, $u+1|v^g$. It is not possible to make perfect power by $w \geq 2$, as we have then two shown factors factorizing differently with gcd either 1 or 2, we need perfect power factors such that for the gcd = 1 we have $u^w - 1 = a^g$ and $u^w + 1 = b^g$, two more smaller Catalan- Mihăilescu equations (leading to infinite descent), moreover we then have three consecutive integers, a^g, u^w, b^g being perfect powers, two of the same exponent (for $a, b > 1$, minimum gap $b^g - a^g = (b-a)(b^{g-1} + \dots + a^{g-1}) \geq b^{g-1} + \dots + a^{g-1} \geq b+a$), which is absurd; only possibility with gcd = 1 is when a factor is non-contributory $u^w - 1 = 1$, and $u = 2, w = 1$ making $u+1|v^g$, a trivial $g = 1$ and $v^g = u+1 = 3$, the equation (2.2) becomes a trivial, $2^2 = 3 + 1$; for the gcd = 2 the product of the factors will be of the form of $2a^g \cdot 2b^g = 2^2 a^g b^g$ then $g = 2$ but powers of the same exponent, a^g, b^g are consecutive integers which is absurd unless $g = 1$ trivial, $v = 4ab$.

(ii)Relating lemma 2.5 to Catalan- Mihăilescu equation we have,

$$u^{2w+1} = (u+1)z - 1 = v^g - 1 \tag{2.3}$$

or adding 1 to (2.3) we have,

$$v^g = (u+1)z = u^{2w+1} + 1 = (u+1)(u^{2w} - \dots + 1) = (u+1)(u^{2w-1}(u-1) \dots + 1)$$

The second factor, is always odd because it has odd number of terms, the last being 1, signs being alternating, the 1st and last terms have positive signs, for $u > 1$ the second factor is not divisible by u , for $u > 2$ the second factor is not divisible by either u or $u-1$, only divisible by $u+1$ when $u = 2, u-1 = 1, w = 1$, and $u^{2w-1}(u-1) \dots + 1 = u(u-1) + 1 = u+1$. It is not possible to make perfect power by $w > 1$, odd exponent $2w+1 > 3$, as we have then two co-prime factors $(u+1) < (u^3(u-1) + u(u-1) + 1) = (u^4 - u^3 + u^2 - u + 1) \leq (u^{2w} - \dots + 1)$; only possibility is $u = 2, w = 1, (u+1)(u+1) = (u+1)^2 = v^g, v = 2+1 = 3, g = 2$, from equation (2.3) we have, the only non-trivial equation, $3^2 = 2^3 + 1$. \square

As before the proof by Mihăilescu, then Catalan conjecture had been verified for very big numbers, for which the number with the bigger base of the consecutives and smaller exponent would be smaller because, by their natural logarithms, $\ln(u+1)^w = w \ln(u+1) < w \ln u + \ln u = \ln u^{w+1}$ so, $(u+1)^w < u^{w+1}$ then for big numbers, it could be, $u^{w+1} - (u+1)^w = 1$ or, $(u+1)^w = u^{w+1} - 1 = (u-1)(u^w + \dots + 1)$ which is not possible as sides have un-shared factors unless $w = 1, u = 2$. Moreover, when $s > t > u \geq 2$ we have, $\log_u \frac{t^s}{s^t} = \log_u t^s - \log_u s^t = s \log_u t - t \log_u s > 0 = \log_u 1$. Only exception, $3 \log_2 2 - 2 \log_2 3$. So, $\frac{t^s}{s^t} > 1$ or, $t^s > s^t$.

3. CONCLUSION

Catalan's Conjecture in number theory is one of those mathematical problems that are very easy to formulate but extremely hard to solve[1]. This conjecture remained unproven since 1844 till 2002.[1, 6] In this article we provided some elementary analyses of integer powers, and in that light we proved Catalan- Mihăilescu Theorem.

ACKNOWLEDGMENT

Those who allowed me hard-found time to do this work.

REFERENCES

- [1] Metsänkylä T., Catalan's Conjecture: Another Old Diophantine Problem Solved. Bulletin (New Series) of the American Mathematical Society, (2003) Vol. 41, Iss. 1, P. 43–57.
- [2] Wikipedia contributors. Catalan's conjecture. Wikipedia, the Free Encyclopedia. URL: https://en.wikipedia.org/wiki/Catalan's_conjecture.
- [3] Bilu Y. F., Bugeaud Y., Mignotte M., The Problem of Catalan. Springer, (2014).
- [4] Catalan E., Note extraite d'une lettre adressée à l'éditeur. J. Reine Angew. Math. (1844) Vol. 27, P. 192.
- [5] Ribenboim P., Catalan's Conjecture. Academic Press, Boston, (1994).
- [6] Preda M., Primary Cyclotomic Units and a Proof of Catalan's Conjecture. J. Reine Angew. Math. (2004) Vol. 572, P. 167–195.

Syed Abdul Kader,
Department of Endocrinology,
Sher-E-Bangla Medical College,
Barisal, Bangladesh
e-mail: skdr0002@gmail.com