PROOF OF FERMAT'S CONJECTURE IN JUST A FEW LINES

Atsu DEKPE
Mathematics Department,
University of Lome,
P.O. Box 1515 Lome,
TOGO,
estatchala@gmail.com

July 24, 2024

Abstract: We present in this paper a formula for decomposing a power of an integer into a product of consecutive integers and its properties. We also discuss properties of some specific vectors (polynomials). By using these concepts, we provide simple proofs for both of Fermat's theorems. Furthermore, the proof of the great Fermat theorem is accessible to all students who have studied the notion of vector space.

Keywords: vector space, vector

1 Introduction

The Fermat's conjecture was proved by Andrew Wiles between 1993 and 1995. However, as it has been the case for other problems in the history of mathematics, exploring alternative paths that may lead to different proofs is not without interest, especially since in this case we employ basic concepts. We first present the formula for decomposing a power of an integer into a product of consecutive integers, its multinomial case, its properties, and the proof of Fermat's little theorem. We also examine the property of some specific polynomials to finally provide a proof of Fermat's conjecture.

2 Formula for Decomposing Integer Powers into Sums

2.1 Theorem (main)

Let n be a integer and p be a non-zero natural number.

$$n^p = \sum_{k=1}^{p} \alpha_p^k A_n^k \quad (2.1)$$

Where $A_n^k = n(n-1)...(n-k+1)$ (2.2) (Read Arrangement of k out of n if $n > 0$)

$$\alpha_p^k = \frac{1}{(k-1)!} \sum_{i=0}^{k-1} (-1)^i C_{k-1}^i (k-i)^{p-1} \quad (2.3)$$

Table of the first values of α_p^k

p/k	1	2	3	4	5	6	7
1	1						
2	1	1					
3	1	3	1				
4	1	7	6	1			
5	1	15	25	10	1		
6	1	31	90	65	15	1	
7	1	63	301	350	140	21	1

Remark : $\alpha_p^1 = \alpha_p^p = 1$; $\alpha_{p-1}^{k-1} + k\alpha_{p-1}^k = \alpha_p^k$

Proof :
* The equality holds true for p=1
* Let's assume the equality holds true for a non-zero integer k, $k > 1$

$$n^k = \sum_{i=1}^{k} \alpha_k^i A_n^i$$

$$
\begin{aligned}
n^{k+1} &= n \times n^k \\
&= n(\alpha_k^1 A_n^1 + \alpha_k^2 A_n^2 + ... + \alpha_k^{k-1} A_n^{k-1} + \alpha_k^k A_n^k) \\
&= \alpha_k^1(n-1+1)A_n^1 + \alpha_k^2(n-2+2)A_n^2 + ... + \alpha_k^{k-1}(n-(k-1)+(k-1))A_n^{k-1} + \\
&\alpha_k^k(n-k+k)A_n^k \\
&= \alpha_k^1(n-1)A_n^1 + \alpha_k^1 A_n^1 + \alpha_k^2(n-2)A_n^2 + 2\alpha_k^2 A_n^2 + ... + \alpha_k^{k-1}(n-(k-1))A_n^{k-1} + \\
&(k-1)\alpha_k^{k-1}A_n^{k-1} + \alpha_k^k(n-k)A_n^k + k\alpha_k^k A_n^k \\
&= \alpha_k^1 A_n^1 + \alpha_k^1 A_n^2 + 2\alpha_k^2 A_n^2 + \alpha_k^2 A_n^3 + ... + (k-1)\alpha_k^{k-1}A_n^{k-1} + \alpha_k^{k-1}A_n^k + k\alpha_k^k A_n^k + \\
&\alpha_k^k A_n^{k+1} \\
&= \alpha_k^1 A_n^1 + (\alpha_k^1 + 2\alpha_k^2)A_n^2 + ... + (\alpha_k^{k-1} + k\alpha_k^k)A_n^k + \alpha_k^k A_n^{k+1} \\
&= \alpha_{k+1}^1 A_n^1 + \alpha_{k+1}^2 A_n^2 + ... + \alpha_{k+1}^k A_n^k + \alpha_{k+1}^{k+1} A_n^{k+1} \\
n^{k+1} &= \sum_{i=1}^{k+1} \alpha_{k+1}^i A_n^i
\end{aligned}
$$

2.2 Theorem (Multinomial case)

Let m and n be two non-zero natural numbers and $x_1, x_2, ..., x_m$ natural numbers $n \leq x_i$. Then,

$$
(x_1+x_2+...+x_m)^n = \sum_{k=1}^{n} \alpha_n^k \sum_{k_1+k_2+...+k_m=k} \binom{k}{k_1, k_2, ..., k_m} A_{x_1}^{k_1} A_{x_2}^{k_2} ... A_{x_m}^{k_m} \quad (2.4)
$$

Proof

Let $a = x_1 + x_2 + ... + x_m \quad (1)$
By substituting (1) into (2.1), we have:

$$
(x_1 + x_2 + ... + x_m)^n = \sum_{k=1}^{n} \alpha_n^k A_{(x_1+x_2+...+x_m)}^k
$$

Where $A_{(x_1+x_2+...+x_m)}^k = \sum_{k_1+k_2+...+k_m=k} \binom{k}{k_1, k_2, ..., k_m} A_{x_1}^{k_1} A_{x_2}^{k_2} ... A_{x_m}^{k_m}$ see [1] and [6]

Then $(x_1+x_2+...+x_m)^n = \sum_{k=1}^{n} \alpha_n^k \sum_{k_1+k_2+...+k_m=k} \binom{k}{k_1, k_2, ..., k_m} A_{x_1}^{k_1} A_{x_2}^{k_2} ... A_{x_m}^{k_m}$

Table of the first values of α_p^k(mod p) (p is a prime number)

p/k	1	2	3	4	5	6	7
1	1						
2	1	1					
3	1	0	1				
4	1	7	6	1			
5	1	0	0	0	1		
6	1	31	90	65	15	1	
7	1	0	0	0	0	0	1

2.3 Proposition

Let p be a prime number, $p>$ 2, and k be a natural number such that $1< k< p$, then $\alpha_p^k \equiv 0 \pmod{p}$

Proof

$\alpha_p^k = \dfrac{1}{(k-1)!}\sum_{i=0}^{k-1}(-1)^i C_{k-1}^i (k-i)^{p-1}$

$(k-1)!\alpha_p^k = \sum_{i=0}^{k-1}(-1)^i C_{k-1}^i (k-i)^{p-1}$

$(k-1)!\alpha_p^k = p \times n$, then p divides $(k-1)!\alpha_p^k$. But p is prime with (k-1)!. Then, according to Gauss theorem, p divides α_p^k.

3 Simple proof of Fermat's little theorem

Theorem

Let p be a prime integer, for any integer n, we have: $n^p \equiv n \pmod{p}$

Proof

From (2.1), we have:

$n^p = n + \sum_{k=2}^{p} \alpha_p^k A_n^k$

$n^p \equiv n \pmod{p}$ because $\sum_{k=2}^{p} \alpha_p^k A_n^k \equiv 0 \pmod{p}$

4 Study on Polynomials

Notation: Throughout the following $P_n(a) = 1 + a + ... + a^n$

4.1 Theorem (main)

Let a and n be natural numbers such that $a > n > 1$

$$P_n(a) = \sum_{k=1}^{n+1} \frac{k}{(a-1)} P_n(k+1) \sum_{i=0}^{n+1-k} (-1)^i C_{k+i}^i C_{a-1}^{k+i} \quad (4.1)$$

change of script:

$$\begin{aligned} \alpha_p^k &= \frac{1}{(k-1)!} \sum_{i=0}^{k-1} (-1)^i C_{k-1}^i (k-i)^{p-1} \quad see\ (2.3) \\ &= \frac{1}{(k-1)!} \sum_{i=0}^{k-1} (-1)^i C_{k-1}^i (k-i)^{p-1} - \frac{1}{(k-1)!} \sum_{i=0}^{k-1} (-1)^i C_{k-1}^i \end{aligned}$$

$$\alpha_p^k = \frac{1}{(k-1)!} \sum_{i=0}^{k-1} (-1)^i C_{k-1}^i [(k-i)^{p-1} - 1] \quad (4.2)$$

Proof

$$
\begin{aligned}
P_n(a) &= 1 + a + ... + a^n \\
&= \frac{1}{a(a-1)}(a^{n+2} - a) \\
&= \frac{1}{a(a-1)}(a + \alpha_{n+2}^2 A_a^2 + \alpha_{n+2}^3 A_a^3 + ... + \alpha_{n+2}^{n+1} A_a^{n+1} + \alpha_{n+2}^{n+2} A_a^{n+2} - a) \quad see\ (2.1) \\
&= \frac{1}{(a-1)}(\alpha_{n+2}^2 A_{a-1}^1 + \alpha_{n+2}^3 A_{a-1}^2 + ... + \alpha_{n+2}^{n+1} A_{a-1}^n + \alpha_{n+2}^{n+2} A_{a-1}^{n+1}) \\
&= \frac{1}{(a-1)}[\frac{1}{1!}[C_1^0(2^{n+1}-1)]A_{a-1}^1 + \frac{1}{2!}[C_2^0(3^{n+1}-1) - C_2^1(2^{n+1}-1)]A_{a-1}^2 \\
&+ ... + \frac{1}{n!}[C_n^0((n+1)^{n+1}-1) - C_n^1(n^{n+1}-1) + ...+ \\
&(-1)^{n-1}C_n^{n-1}(2^{n+1}-1)]A_{a-1}^n + \frac{1}{(n+1)!}[C_{n+1}^0((n+2)^{n+1}-1) \\
&- C_{n+1}^1((n+1)^{n+1}-1) + ... + (-1)^n C_{n+1}^n(2^{n+1}-1)]A_{a-1}^{n+1}] \ \ see\ (4.2) \\
&= \frac{1}{(a-1)}[C_1^0(2^{n+1}-1)C_{a-1}^1 + [C_2^0(3^{n+1}-1) - C_2^1(2^{n+1}-1)]C_{a-1}^2 \\
&+ ... + [C_n^0((n+1)^{n+1}-1) - C_n^1(n^{n+1}-1) + ...+ \\
&(-1)^{n-1}C_n^{n-1}(2^{n+1}-1)]C_{a-1}^n + [C_{n+1}^0((n+2)^{n+1}-1) \\
&- C_{n+1}^1((n+1)^{n+1}-1) + ... + (-1)^n C_{n+1}^n(2^{n+1}-1)]C_{a-1}^{n+1}] \\
&= \frac{1}{(a-1)}[(2^{n+1}-1)[C_1^0C_{a-1}^1 - C_2^1C_{a-1}^2 + ... + (-1)^{n-1}C_n^{n-1}C_{a-1}^n + (-1)^n C_{n+1}^n C_{a-1}^{n+1}] \\
&+ (3^{n+1}-1)[C_2^0C_{a-1}^2 - C_3^1C_{a-1}^3 + ... + (-1)^{n-2}C_n^{n-2}C_{a-1}^n + (-1)^{n-1}C_{n+1}^{n-1}C_{a-1}^{n+1}] \\
&+ ... + ((n+1)^{n+1}-1)[C_n^0C_{a-1}^n - C_{n+1}^1C_{a-1}^{n+1}] + ((n+2)^{n+1}-1)C_{n+1}^0C_{a-1}^{n+1}] \\
P_n(a) &= \sum_{k=1}^{n+1} \frac{k}{(a-1)} P_n(k+1) \sum_{i=0}^{n+1-k} (-1)^i C_{k+i}^i C_{a-1}^{k+i}
\end{aligned}
$$

4.2 Theorem (main)

Let a be an integer such that $a < -1$, and let n be a non-zero natural number.

$$P_n(a) = \sum_{k=1}^{n+1}(-1)^k \frac{k}{(a-1)} P_n(k+1) \sum_{i=0}^{n+1-k} C_{k+i}^i C_{(k+i-a)}^{k+i} \quad (4.3)$$

Proof

$$
\begin{aligned}
P_n(a) &= 1 + a + ... + a^n \\
&= \frac{1}{a(a-1)}(a^{n+2} - a) \\
&= \frac{1}{a(a-1)}(a + \alpha^2_{n+2}A^2_a + \alpha^3_{n+2}A^3_a + ... + \alpha^{n+1}_{n+2}A^{n+1}_a + \alpha^{n+2}_{n+2}A^{n+2}_a - a) \quad see\ (2.1) \\
&= \frac{1}{(a-1)}(\alpha^2_{n+2}A^1_{a-1} + \alpha^3_{n+2}A^2_{a-1} + ... + \alpha^{n+1}_{n+2}A^n_{a-1} + \alpha^{n+2}_{n+2}A^{n+1}_{a-1}) \\
&= \frac{1}{(a-1)}((-1)^1\alpha^2_{n+2}A^1_{1-a} + (-1)^2\alpha^3_{n+2}A^2_{2-a} + ... + (-1)^n\alpha^{n+1}_{n+2}A^n_{n-a} + (-1)^{n+1}\alpha^{n+2}_{n+2}A^{n+1}_{n+1-a}) \\
&= \frac{1}{(a-1)}[(-1)^1\frac{1}{1!}[(-1)^0C^0_1(2^{n+1}-1)]A^1_{1-a} + (-1)^2\frac{1}{2!}[(-1)^0C^0_2(3^{n+1}-1) \\
&+ (-1)^1C^1_2(2^{n+1}-1)]A^2_{2-a} + ... + (-1)^n\frac{1}{n!}[(-1)^0C^0_n((n+1)^{n+1}-1) + (-1)^1C^1_n(n^{n+1}-1) \\
&+ ... + (-1)^{n-1}C^{n-1}_n(2^{n+1}-1)]A^n_{n-a} + (-1)^{n+1}\frac{1}{(n+1)!}[(-1)^0C^0_{n+1}((n+2)^{n+1}-1) \\
&+ (-1)^1C^1_{n+1}((n+1)^{n+1}-1) + ... + (-1)^nC^n_{n+1}(2^{n+1}-1)]A^{n+1}_{n+1-a}] \ \ see\ (4.2) \\
&= \frac{1}{(a-1)}[(-1)^1(-1)^0C^0_1(2^{n+1}-1)C^1_{1-a} + (-1)^2[(-1)^0C^0_2(3^{n+1}-1) + (-1)^1C^1_2(2^{n+1}-1)]C^2_{2-a} \\
&+ ... + (-1)^n[(-1)^0C^0_n((n+1)^{n+1}-1) + (-1)^1C^1_n(n^{n+1}-1) + ...+ \\
&(-1)^{n-1}C^{n-1}_n(2^{n+1}-1)]C^n_{n-a} + (-1)^{n+1}[(-1)^0C^0_{n+1}((n+2)^{n+1}-1) \\
&+ (-1)^1C^1_{n+1}((n+1)^{n+1}-1) + ... + (-1)^nC^n_{n+1}(2^{n+1}-1)]C^{n+1}_{n+1-a}] \\
&= \frac{1}{(a-1)}[(2^{n+1}-1)[(-1)^1(-1)^0C^0_1C^1_{1-a} + (-1)^2(-1)^1C^1_2C^2_{2-a} + ... + (-1)^n(-1)^{n-1}C^{n-1}_nC^n_{n-a} \\
&+ (-1)^{n+1}(-1)^nC^n_{n+1}C^{n+1}_{n+1-a}] + (3^{n+1}-1)[(-1)^2(-1)^0C^0_2C^2_{2-a} + (-1)^3(-1)^1C^1_3C^3_{3-a} + ...+ \\
&(-1)^n(-1)^{n-2}C^{n-2}_nC^n_{n-a} + (-1)^{n+1}(-1)^{n-1}C^{n-1}_{n+1}C^{n+1}_{n+1-a}] + ...+ \\
&((n+1)^{n+1}-1)[(-1)^n(-1)^0C^0_nC^n_{n-a} + (-1)^{n+1}(-1)^1C^1_{n+1}C^{n+1}_{n+1-a}]+ \\
&((n+2)^{n+1}-1)(-1)^{n+1}(-1)^0C^0_{n+1}C^{n+1}_{n+1-a}] \\
&= \frac{1}{(a-1)}[(-1)^1(2^{n+1}-1)[(-1)^{2\times0}C^0_1C^1_{1-a} + (-1)^{2\times1}C^1_2C^2_{2-a} + ... + (-1)^{2(n-1)}C^{n-1}_nC^n_{n-a} \\
&+ (-1)^{2n}C^n_{n+1}C^{n+1}_{n+1-a}] + (-1)^2(3^{n+1}-1)[(-1)^{2\times0}C^0_2C^2_{2-a} + (-1)^{2\times1}C^1_3C^3_{3-a} + ...+ \\
&(-1)^{2(n-2)}C^{n-2}_nC^n_{n-a} + (-1)^{2(n-1)}C^{n-1}_{n+1}C^{n+1}_{n+1-a}] + ... + (-1)^n((n+1)^{n+1}-1)[(-1)^{2\times0}C^0_nC^n_{n-a} \\
&+ (-1)^{2\times1}C^1_{n+1}C^{n+1}_{n+1-a}] + (-1)^{n+1}((n+2)^{n+1}-1)(-1)^{2\times0}C^0_{n+1}C^{n+1}_{n+1-a}]
\end{aligned}
$$

$$P_n(a) = \sum_{k=1}^{n+1}(-1)^k\frac{k}{(a-1)}P_n(k+1)\sum_{i=0}^{n+1-k}C^i_{k+i}C^{k+i}_{(k+i-a)}$$

We note that $P_n(k+1)$, $1 \le k \le n+1$ forms basis for $\mathbf{R_n}$

Proof

From (4.1) $P_n(k+1)$, $1 \leq k \leq n+1$ is a generating family

$$P_n(a) = 0 \iff \sum_{k=1}^{n+1} \frac{k}{(a-1)} P_n(k+1) \sum_{i=0}^{n+1-k} (-1)^i C_{k+i}^i C_{a-1}^{k+i} = 0$$

$$\Rightarrow \sum_{i=0}^{n+1-k} (-1)^i C_{k+i}^i C_{a-1}^{k+i} = 0,\ 1 \leq k \leq n+1$$

$\Rightarrow P_n(k+1)$, $1 \leq k \leq n+1$ is linearly independent family

5 Proof of Fermat's conjecture

5.1 Conjecture recall

Consider the equation: $x^n + y^n = z^n \quad (5.1)$

For any integer $n > 2$, Fermat conjectured that there exist no triplets $x \in \mathbf{N}^*$, $y \in \mathbf{N}^*$, $z \in \mathbf{N}^*$ satisfying the relation (5.1).

We assume $0 < x < y < z$

$x + y \equiv z (\text{mod } n) \iff x + y = kn + z (k \in \mathbf{N}^*)$

$\Rightarrow x > kn$

5.2 Proof

Let's reason by contradiction:

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

$x^n - 1 + y^n - 1 = z^n - 1 - 1$

$$\sum_{k=1}^{n} kP_{n-1}(k+1) \sum_{i=0}^{n-k} (-1)^i C_{k+i}^i C_{x-1}^{k+i} + \sum_{k=1}^{n} kP_{n-1}(k+1) \sum_{i=0}^{n-k} (-1)^i C_{k+i}^i C_{y-1}^{k+i} =$$

$$\sum_{k=1}^{n} kP_{n-1}(k+1) \sum_{i=0}^{n-k} (-1)^i C_{k+i}^i C_{z-1}^{k+i} - 1 \quad see \quad (4.1)$$

As $P_{n-1}(k+1)$; $1 \leq k \leq n$ is a base :

$$\Rightarrow \begin{cases} C_{x-1}^{k+i} + C_{y-1}^{k+i} = C_{z-1}^{k+i}; & 1 \leq k \leq n; \quad 0 \leq i \leq n-k \\ 0 = -1 \ \ impossible \end{cases}$$

Hence, the equation has no solution.

6 Conclusion

In this study, we derived a formula expressing an integer power as a product of consecutive integers, and its generalization for natural numbers, which enables us to provide a simple proof of Fermat's Little Theorem. The identities presented in Theorems (4.1) and (4.3) constitute a decomposition of certain specific polynomials in the base $\mathbf{R_n}$. Furthermore, Theorem (4.1) allows for a straightforward proof of Fermat's conjecture.

REFERENCE

[1] A Dekpe. Mutinomial development. 2023;1-18 [Google Scholar] [Crossref].
[2] A.J.Best; C.Birkbeek, R.Brasca and E.Boidi; Fermat's Last theorem for regular primes arxiv: 2305.08955 v1[CS.LO] 15 May 2023.
[3] Andrew Wiles, Modular elliptic curves and Fermat's last Théorème, Annal of mathematics, 142, 443-551, 1995
[4] Cai, T., Chen, D., Zhang, Y. (2015). A new generalization of Fermat's Last Theorem, J. of Number Theory, 149, pp. 33-45.
[5] Cox, Darrell. (2020). Fermat's Congruence Modulo a Prime-Power.
[6] Dekpe A. A probabilistic proof of the multinomial theorem following the number A_n^p . J Pure Appl Math. 2023; 7(3):202-203.
[7]De Pedis, D. (2012). Polynomial representation of Fermat's Last Theorem, www.arXiv.org.
[8] Faltings, G. (1995). The Proof of Fermat's Last Theorem by R. Taylor and A. Wiles, Notices of the American Mathematical Society, 42(7), pp. 743-746.
[9] Hurwitz,A. Über die diophantische Gleichung $x^3y + y^3z + z^3x = 0$. Math, Annalen,65,1908.
[10] Mohamed Sghiar. LA PREUVE DE LA CONJECTURE ABC. JOSR Journal of Mathematic(JOSR-JM), 2018, 14(4),pp.22-26.
[11] Nemron, I.A.G. (2012). A Complete Simple Proof of the Fermat's Last Conjecture, Int. Mathematical Forum, 7(20), pp. 953-971.
[12] Sghiar, Mohamed. (2016). Une preuve relativiste du Théorème de Fermat-Wiles.