Iğdır Üniversitesi Fen Bilimleri Enstitüsü Dergisi
Iğdır University Journal of the Institute of Science and Technology

Catalan Numbers and Modular Arithmetic

Engin ÖZKAN[1] Sedat DERVİŞOĞLU[1]

ABSTRACT: For prime numbers, we examined Catalan numbers in modula arithmetic and proved some theorems about them. Also, some theorems concerning with Catalan numbers for mod p, mod p^2 and mod p^3 such that p were given.

Keywords: Wolstenholme's theorem, Lucas theorem, prime numbers

Katalan Sayılar ve Modüler Aritmetik

ÖZET: Modüler aritmetikte Katalan sayıları asal sayılar için incelenmiş ve onunla ilgili bazı teoremler ispatlanmıştır. Ayrıca, p asal sayı olmak üzere, mod p, mod p^2 ve mod p^3 için Katalan sayılarla ilgili teoremler verilmiştir.

Anahtar kelimeler: Wolstenholme's theorem, Lucas teoremi, asal sayılar

Cilt: 2, Sayı: 4, Sayfa: 63-66, 2012
Volume: 2, Issue:4, pp: 63-66, 2012

[1] Erzincan University, Faculty of Arts and Science, Department of Mathematics, Erzincan, Turkey
Sorumlu yazar/Corresponding author: Engin ÖZKAN, eozkan@erzincan.edu.tr

Geliş tarihi / *Received:* 20.06.2012
Kabul tarihi / *Accepted:* 01.11.2012

INTRODUCTION

Catalan numbers, a sequence of numbers, are usually used in computer technology and combinatorics which is a branch of mathematics. Technological developments are known to be proportional with mathematics. In 2002, Catalan numbers are generalized by Pantelimon Stanica (Stanica, 2003) and are examined for modula 4 and modula 8 by Sen-Peng Eu, Shu-Chung Liu, Yeong-Nan Yeh (Eu et al., 2008). We examined Catalan numbers in modula arithmetic and we introduced some theorems about Catalan numbers. Our results provide scientist come to conclusion exact results in a short time.

MATERIALS AND METHODS

We use some properties of Catalan numbers and modula arithmetic. We also use Lucas theorem and Wolstenholme's theorem to prove some of our theorems in the paper. Therefore, some definitions and properties of Catalan numbers are to be given here.

Definition: In combinatorial mathematics, the Catalan numbers form a sequence of natural numbers that occur in various counting, often involving recursively defined objects. They are named after the Belgian mathematician Charles Catalan (1814 – 1894), (Foot et al., 2004).

The n^{th} Catalan number is given directly in terms of binomial coefficients by:

For $n \geq 0$;

$$C_n = \frac{1}{n+1}\binom{2n}{n} = \frac{(2n)!}{(n+1)!n!} \qquad (1)$$

and

$$\binom{2n}{n+1} = \frac{n}{n+1}\binom{2n}{n} \qquad (2)$$

Also If we use the equal, we have that

$$C_n = \binom{2n}{n} - \binom{2n}{n+1} \qquad (3)$$

This shows that C_n is an integer number, which is not immediately obvious from the first formula given.

Applications in combinatorics;

- Re-interpreting the symbol X as an open parenthesis and Y as a close parenthesis, C_n counts the number of expressions containing n pairs of parentheses which are correctly matched:
- Successive applications of a binary operator can be represented in terms of a full binary tree. (A rooted binary tree is *full* if every vertex has either two children or no children.)
- C_n is the number of monotonic paths along the edges of a grid with $n \times n$ square cells, which do not pass above the diagonal. A monotonic path is one which starts in the lower left corner, finishes in the upper right corner, and consists entirely of edges pointing rightwards or upwards. Counting such paths is equivalent to counting Dyck words: X stands for "move right" and Y stands for "move up".
- C_n is the number of different ways a convex polygon with $n + 2$ sides can be cut into triangles by connecting vertices cwith straight lines
- C_n is the number of permutations of $\{1, ..., n\}$ that avoid the pattern 123 (or any of the other patterns of length 3); that is, the number of permutations with no three-term increasing subsequence. For $n = 3$, these permutations are 132, 213, 231, 312 and 321. For $n = 4$, they are 1432, 2143, 2413, 2431, 3142, 3214, 3241, 3412, 3421, 4132, 4213, 4231, 4312 and 4321.
- C_n is the number of ways that the vertices of a convex $2n$-gon can be paired so that the line segments joining paired vertices do not intersect.

There are several ways of explaining the formula.

If we use any one of given formulas, the sequence can be obtain as shown:

C_0=1, C_1=1, C_2=2, C_3 =5, C_4 =14, C_5 =42, C_6=132, C_7=429, C_8 =1430,…

Now, we will give Lucas Theorem to prove our theorem.

Lucas Theorem: For non-negative integers m and n, and a prime p, the following congruence relation holds;

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p}$$

where;

$$m = m_k p^k + m_{k-1} p^{k-1} + ... + m_1 p + m_0$$

and

$$n = n_k p^k + n_{k-1} p^{k-1} + ... + n_1 p + n_0$$

are the base p expansions of m and n respectively.

Now, another theorem concerning with Catalan numbers will be given here.

Wolstenholme's Theorem: If p is a prime and p>3 we have a equal that

$$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3}$$

Therefore, Wolstenholme's theorem states that for primes p ≥ 5 we have the congruence;

$$\binom{2p}{p} \equiv 2 \pmod{p^3} \text{ and so } \binom{2p}{p} \equiv 2 \pmod{p^2}$$

(Wolstenholme, 1862)

Now, we will give our theorems.

RESULTS AND DISCUSSION

Theorem 1: If p is a prime number then $C_p \equiv 2 \pmod{p}$.

Proof: Let us apply Lucas Theorem to Theorem 1;

It is obvious that

$m = 2p$ and $n = p$,

also

$m_1 = 2,\ m_0 = 0$ and $n_1 = 1,\ n_0 = 0$.

By Lucas Theorem, we can write that.

$$\binom{2p}{p} \equiv \prod_{i=0}^{1} \binom{m_1}{n_1} \pmod{p} \equiv \binom{m_0}{n_0}\binom{m_1}{n_1} \pmod{p}$$

If we write values of m_0, m_1, n_0 and n_1 in the equal then we have that

$$\binom{2p}{p} \equiv \binom{0}{0}\binom{2}{1} \pmod{p} \equiv 2 \pmod{p}$$

also

$$C_p = \frac{1}{p+1}\binom{2p}{p} \equiv a.b \pmod{p}$$

If we write this equal in this way, it will confirm the equal. There are values of a and b such that

$$\frac{1}{p+1} \equiv a \pmod{p}$$

and

$$\binom{2p}{p} \equiv b \pmod{p}$$

By Lucas Theorem we obtain that $b = 2$. Now, we will find "a";

$$\frac{1}{p+1} \equiv a \pmod{p}$$

If we multiply the last congruence by $(1- p^2)$ and use $(1-p^2) = (1-p)(1+p)$ then we find $a = 1$.

$$C_p = \frac{1}{p+1}\binom{2p}{p} \equiv 1.2 \pmod{p} \equiv 2 \pmod{p}$$

we are done.

Theorem 2: If p is a n odd prime number and $p \geq 3$ then $C_p \equiv 2 - 2p \pmod{p^2}$.

Proof: As similarly Theorem 1;

$$C_p \equiv 2 - 2p \pmod{p^2}$$

$$C_p = \frac{1}{p+1}\binom{2p}{p} \equiv a.b \pmod{p^2}$$

If we write the equal in this way, it will confirm followings,

$$\frac{1}{p+1} \equiv a \pmod{p^2}$$

and

$$\binom{2p}{p} \equiv b \pmod{p^2}$$

The values of *a* and *b* will be found. Also, we found that $b = 2$ with Wolstenholme's theorem now let us find value of *a*;

$$\frac{1}{p+1} \equiv a \pmod{p^2}$$

If we make use of the same way as we did in previous theorem, If we multiply with (1- p^2) and if we use this equal:

$$(1 - p^2) = (1 - p)(1 + p)$$

It can be clearly seen that equal is *a=(1*-p) .In this situation we find this;

$$C_p = \frac{1}{p+1}\binom{2p}{p} \equiv (1\text{-p}).2 \pmod{\text{p}^2} \equiv 2\text{ - 2p}(\text{mod}\text{p}^2)$$

Theorem 3: If p is a prime number and $p \geq 7$ then $\text{C}_\text{p} \equiv 2.(\text{p}^2\text{-p+1}) \pmod{\text{p}^3}$.

Proof: As in previous proof:

$$C_p = \frac{1}{p+1}\binom{2p}{p}$$

If we write this equal like that

$$C_p = \frac{1}{p+1}\binom{2p}{p} \equiv \text{a.b} \pmod{\text{p}^3}$$

It will prove this equal

$$\frac{1}{p+1} \equiv a \pmod{p^3}$$

and

$$\binom{2p}{p} \equiv b \pmod{p^3}$$

We can find values of *a* and *b*. It can be found by using Wolstenholme's theorem that *b*=2. Now let us find value of *a*;

$$\frac{1}{p+1} \equiv a \pmod{p^3}$$

If we make use of the same way as we did in previous theorem, If we multiply with (1 +p^3) and if we use this equal;

$$(1 + p^3) = (1 + p)(p^2 - p + 1)$$

It can be clearly seen that $a = p^2 - p + 1$. In this situation we find this;

$$C_p = \frac{1}{p+1}\binom{2p}{p} \equiv (p^2 - p + 1).2 \pmod{p^3}$$
$$\equiv 2 - 2p \pmod{p^2}$$

CONCLUSION

We examined Catalan numbers in modula arithmetic for p, which is a prime, and we researched Wolstenholme's theorem and Lucas's theorem. It is widely believed that Catalan Numbers are used in department of Computer Science and Geometry. Our results provide scientist come to conclusion exact results in a short time rather than dealing with lots of processes.

REFERENCES

Dummit, D.S., Foote, R.M., 2004. Abstract algebra. Third Edition, John Wiley and Sons, Inc., United States.

Stanica, P., 2003. p^q-Catalan numbers and squarefree binomial coefficients. Journal of Number Theory, 100: 203-216.

Wolstenholme, J., 1862. On certain properties of prime numbers, Quarterly Journal of Mathematics 5: 3539.

Yeh, Y., Eu, S., Liu, S., 2008. Catalan and Motzkin numbers modulo 4 and 8. European Journal of Combinatorics, 29: 1449-1466.