CATALAN NUMBERS MODULO A PRIME POWER

Yong-Gao Chen[1]
School of Mathematical Sciences and Institute of Mathematics, Nanjing Normal University, Nanjing, P. R. CHINA
ygchen@njnu.edu.cn

Wen Jiang
School of Mathematical Sciences and Institute of Mathematics, Nanjing Normal University, Nanjing, P. R. CHINA

Received: 9/6/12, Accepted: 5/1/13, Published: 6/14/13

Abstract

Let $C_n = (2n)!/((n+1)!n!)$ be the n-th Catalan number. It is proved that for any odd prime p and integers a, k with $0 \le a < p$ and $k > 0$, if $0 \le a < (p+1)/2$, then the Catalan numbers $C_{p^1-a}, \ldots, C_{p^k-a}$ are all distinct modulo p^k, and the sequence $(C_{p^n-a})_{n\ge 1}$ modulo p^k is constant from $n = k$ on; if $(p+1)/2 \le a < p$, then the Catalan numbers $C_{p^1-a}, \ldots, C_{p^{k+1}-a}$ are all distinct modulo p^k, and the sequence $(C_{p^n-a})_{n\ge 1}$ modulo p^k is constant from $n = k+1$ on. The similar conclusion is proved for $p = 2$ recently by Lin.

1. Introduction

Let $C_n = (2n)!/((n+1)!n!)$ be the n-th Catalan number. In 2011, Lin [4] proved a conjecture of Liu and Yeh by showing that for all $k \ge 2$, the Catalan numbers $C_{2^1-1},\ldots,C_{2^{k-1}-1}$ are all distinct modulo 2^k, and the sequence $(C_{2^n-1})_{n\ge 1}$ modulo 2^k is constant from $n = k-1$ on. For $k = 2, 3$, this is proved by Eu, Liu and Yeh [2]. In this paper, the following result is proved.

Theorem 1. *Let p be an odd prime and a, k be two integers with $0 \le a < p$ and $k > 0$. Then*

(i) for $0 \le a < \frac{1}{2}(p+1)$, the Catalan numbers $C_{p^1-a}, \ldots, C_{p^k-a}$ are all distinct modulo p^k, and the sequence $(C_{p^n-a})_{n\ge 1}$ modulo p^k is constant from $n = k$ on;

(ii) for $\frac{1}{2}(p+1) \le a < p$, the Catalan numbers $C_{p^1-a}, \ldots, C_{p^{k+1}-a}$ are all distinct modulo p^k, and the sequence $(C_{p^n-a})_{n\ge 1}$ modulo p^k is constant from $n = k+1$ on.

[1] This work was supported by the National Natural Science Foundation of China, Grant No 11071121.

2. Proof of the Theorem

We begin with the following lemmas.

Lemma 1. ([1]) *For any odd prime p and any positive integer k, we have*

$$p \nmid C_{p^k-1}.$$

Lemma 2. ([3, Theorem 129]) *If p is an odd prime and k is a positive integer, then*

$$\prod_{\substack{0<d<p^k \\ (d,p)=1}} d \equiv -1 \pmod{p^k}.$$

Lemma 3. *Let p be an odd prime, and a, i be integers with $0 \le a < p$ and $i > 0$. Then*

(i) for $0 \le a < \frac{1}{2}(p+1)$, we have

$$C_{p^{i+1}-a} \equiv C_{p^i-a} \pmod{p^i}, \quad C_{p^{i+1}-a} \not\equiv C_{p^i-a} \pmod{p^{i+1}};$$

(ii) for $\frac{1}{2}(p+1) \le a < p$, we have

$$C_{p^{i+1}-a} \equiv C_{p^i-a} \pmod{p^{i-1}}, \quad C_{p^{i+1}-a} \not\equiv C_{p^i-a} \pmod{p^i}.$$

Proof. First we deal with the case $a = 1$.

Define $\tau_p(n) = n/p^\alpha$ for $p^\alpha \mid n$ and $p^{\alpha+1} \nmid n$. By Lemma 1, we have

$$2(2p^{i+1}-1)C_{p^{i+1}-1} = \frac{2 \cdot (2p^{i+1}-1)!}{p^{i+1}!(p^{i+1}-1)!} = \frac{\tau_p(2 \cdot (2p^{i+1}-1)!)}{\tau_p(p^{i+1}!(p^{i+1}-1)!)} = \frac{\tau_p((2p^{i+1})!)}{(\tau_p(p^{i+1}!))^2}. \quad (1)$$

Similarly, we have

$$2(2p^i-1)C_{p^i-1} = \frac{\tau_p((2p^i)!)}{(\tau_p(p^i!))^2}. \quad (2)$$

Since

$$p^{i+1}! = \prod_{\substack{0<d<p^{i+1} \\ (d,p)=1}} d \cdot \prod_{v=1}^{p^i} vp,$$

by Lemma 2, we have

$$\tau_p(p^{i+1}!) \equiv -\tau_p(p^i!) \pmod{p^{i+1}}. \quad (3)$$

Similarly, we have

$$\tau_p((2p^{i+1})!) \equiv \tau_p((2p^i)!) \pmod{p^{i+1}}. \quad (4)$$

By (1), (2), (3) and (4), we have

$$2(2p^{i+1}-1)C_{p^{i+1}-1} \equiv 2(2p^i-1)C_{p^i-1} \pmod{p^{i+1}}.$$

That is,

$$C_{p^{i+1}-1} \equiv (1-2p^i)C_{p^i-1} \pmod{p^{i+1}}.$$

Now Lemma 3 for $a=1$ follows immediately from Lemma 1 and the above congruence.

If $a=0$, then

$$C_{p^i-a} = C_{p^i} = \frac{(2p^i)!}{p^i!(p^i+1)!} = \frac{(2p^i)(2p^i-1)}{p^i(p^i+1)}C_{p^i-1} = \frac{2(2p^i-1)}{p^i+1}C_{p^i-1}.$$

Thus, by Lemma 1 we have $p \nmid C_{p^i}$. Hence

$$(p^i+1)C_{p^i} = \frac{\tau_p((2p^i)!)}{(\tau_p(p^i!))^2}. \tag{5}$$

Similarly, we have

$$(p^{i+1}+1)C_{p^{i+1}} = \frac{\tau_p((2p^{i+1})!)}{(\tau_p(p^{i+1}!))^2}. \tag{6}$$

By (3)-(6) we have

$$(p^i+1)C_{p^i} \equiv (p^{i+1}+1)C_{p^{i+1}} \pmod{p^{i+1}}.$$

Now Lemma 3 for $a=0$ follows immediately.

Now we assume that $2 \le a < p$. Then

$$\begin{aligned} C_{p^i-a} &= \frac{(2p^i-2a)!}{(p^i-a)!(p^i-a+1)!} \\ &= \frac{(p^i-a+1)\cdots(p^i-1)(p^i-a+2)\cdots p^i}{(2p^i-2a+1)\cdots(2p^i-2)} \cdot \frac{(2p^i-2)!}{(p^i-1)!p^i!} \\ &= \frac{(p^i-a+1)\cdots(p^i-1)(p^i-a+2)\cdots p^i}{(2p^i-2a+1)\cdots(2p^i-2)}\ C_{p^i-1}. \end{aligned} \tag{7}$$

By Lemma 1 we have $p \nmid C_{p^i-1}$ for $i \ge 1$. If $2 \le a < \frac{1}{2}(p+1)$, then, by (7), we have

$$p^i \mid C_{p^i-a}, \quad p^{i+1} \nmid C_{p^i-a}.$$

Similarly, we have

$$p^{i+1} \mid C_{p^{i+1}-a}, \quad p^{i+2} \nmid C_{p^{i+1}-a}.$$

Hence, if $2 \le a < \frac{1}{2}(p+1)$, then

$$C_{p^{i+1}-a} \equiv C_{p^i-a} \pmod{p^i}, \quad C_{p^{i+1}-a} \not\equiv C_{p^i-a} \pmod{p^{i+1}}.$$

If $\frac{1}{2}(p+1) \le a < p$, then, by (7), we have

$$p^{i-1} \mid C_{p^i-a}, \quad p^i \nmid C_{p^i-a}.$$

Similarly, we have

$$p^i \mid C_{p^{i+1}-a}, \quad p^{i+1} \nmid C_{p^{i+1}-a}.$$

Hence, if $\frac{1}{2}(p+1) \le a < p$, then

$$C_{p^{i+1}-a} \equiv C_{p^i-a} \pmod{p^{i-1}}, \quad C_{p^{i+1}-a} \not\equiv C_{p^i-a} \pmod{p^i}.$$

This completes the proof of Lemma 3. □

Proof of Theorem 1. We prove (i). Case (ii) is similar. Assume that $0 \le a < \frac{1}{2}(p+1)$. For any $u \ge v$, by Lemma 3 (i) and $p^v \mid p^u$, we have

$$C_{p^{u+1}-a} \equiv C_{p^u-a} \pmod{p^v}. \tag{8}$$

For $1 \le i < j \le k$, by (8) and Lemma 3 (i) we have

$$C_{p^j-a} \equiv C_{p^{j-1}-a} \equiv \cdots \equiv C_{p^{i+1}-a} \not\equiv C_{p^i-a} \pmod{p^{i+1}}. \tag{9}$$

Since $p^{i+1} \mid p^k$, it follows from (9) that

$$C_{p^j-a} \not\equiv C_{p^i-a} \pmod{p^k}.$$

For $n > k$, by (8) we have

$$C_{p^n-a} \equiv C_{p^{n-1}-a} \equiv \cdots \equiv C_{p^k-a} \pmod{p^k}.$$

This completes the proof of Theorem 1. □

References

[1] R. Alter and K. Kubota, *Prime and prime power divisibility of Catalan numbers,* J. Combin. Theory Ser. A 15 (1973), 243-256.

[2] S.-P. Eu, S.-C. Liu and Y.-N. Yeh, *Catalan and Motzkin numbers modulo 4 and 8,* European J. Combin. 29 (2008), 1449-1466.

[3] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 5th ed., Clarendon Press, Oxford Univ. Press, New York, 1979.

[4] H.-Y. Lin, *Odd Catalan numbers modulo* 2^k*,* Integers 12 (2012), no. 2, 161-165.