

Catalan Numbers Modulo a Prime Power

Larry Shu-Chung Liu

National Hsinchu University of Education, Taiwan

a joint work with Jean C.-C. Yeh (Texas A&M)

In honor of Professor Doron Zeilberger's birthday

Outline

- 1 Some results about $\binom{m}{n}$ during the late 1800
- 2 Some recent works for a prime power modulus
- 3 Our technique
- 4 Catalan numbers modulus 2^k
- 5 Catalan numbers modulus an odd prime power

Outline

- 1 Some results about $\binom{m}{n}$ during the late 1800
- 2 Some recent works for a prime power modulus
- 3 Our technique
- 4 Catalan numbers modulus 2^k
- 5 Catalan numbers modulus an odd prime power

- The *p-adic order* of an integer n is denoted and defined as

$$\omega_p(n) := \max\{\alpha \in \mathbb{N} : p^\alpha | n\}.$$

- The *p-adic order* of an integer n is denoted and defined as

$$\omega_p(n) := \max\{\alpha \in \mathbb{N} : p^\alpha | n\}.$$

- Let $C(m, n)$ be the number of *total carries* for operating $m + n$.

- The *p-adic order* of an integer n is denoted and defined as

$$\omega_p(n) := \max\{\alpha \in \mathbb{N} : p^\alpha | n\}.$$

- Let $C(m, n)$ be the number of *total carries* for operating $m + n$.

Theorem (Kummer, 1852)

$$\omega_p \left(\binom{m+n}{m} \right) = C(m, n).$$

Let p be a fixed prime and n be any integer. Define that

- $[n]_p := \langle \dots n_2 n_1 n_0 \rangle_p$ be the representation of n in the base- p system.

Let p be a fixed prime and n be any integer. Define that

- $[n]_p := \langle \dots n_2 n_1 n_0 \rangle_p$ be the representation of n in the base- p system.
- $|\langle \dots n_2 n_1 n_0 \rangle_p| := n_0 + n_1 p + n_2 p^2 + \dots = n.$

Let p be a fixed prime and n be any integer. Define that

- $[n]_p := \langle \dots n_2 n_1 n_0 \rangle_p$ be the representation of n in the base- p system.
- $|\langle \dots n_2 n_1 n_0 \rangle_p| := n_0 + n_1 p + n_2 p^2 + \dots = n$.

Theorem (Lucas, 1877)

$$\binom{m}{n} \equiv_p \prod_{i \geq 0} \binom{m_i}{n_i}.$$

└ Some results about $\binom{m}{n}$ during the late 1800

└ $\binom{m}{n}/p^\omega \pmod{p}$

Theorem (Anton, 1869; Stickelberger, 1890; Hensel, 1902; and etc)

Given non-negative integers m and n , let $r = m - n$. We have

$$\frac{(-1)^\omega}{p^\omega} \binom{m}{n} \equiv_p \prod_{i \geq 0} \frac{m_i!}{n_i! r_i!},$$

where $\omega = \omega_p(\binom{m}{n})$.

└ Some results about $\binom{m}{n}$ during the late 1800

└ $\binom{m}{n} / p^\omega \pmod{p}$

Theorem (Anton, 1869; Stickelberger, 1890; Hensel, 1902; and etc)

Given non-negative integers m and n , let $r = m - n$. We have

$$\frac{(-1)^\omega}{p^\omega} \binom{m}{n} \equiv_p \prod_{i \geq 0} \frac{m_i!}{n_i! r_i!},$$

where $\omega = \omega_p(\binom{m}{n})$.

■ Notice that

$$r_i \equiv_p m_i - n_i - \kappa(m, n, i - 1),$$

where $\kappa(m, n, i - 1)$ is the possible borrow from the i -th place to the $(i - 1)$ -st place when operating $m - n$.

└ Some results about $\binom{m}{n}$ during the late 1800

└ $\binom{m}{n}/p^\omega \pmod{p}$

Theorem (Anton, 1869; Stickelberger, 1890; Hensel, 1902; and etc)

Given non-negative integers m and n , let $r = m - n$. We have

$$\frac{(-1)^\omega}{p^\omega} \binom{m}{n} \equiv_p \prod_{i \geq 0} \frac{m_i!}{n_i! r_i!},$$

where $\omega = \omega_p(\binom{m}{n})$.

■ Notice that

$$r_i \equiv_p m_i - n_i - \kappa(m, n, i - 1),$$

where $\kappa(m, n, i - 1)$ is the possible borrow from the i -th place to the $(i - 1)$ -st place when operating $m - n$.

■ Analogous formulae w.r.t. modulus p^k were recently given by Granville and {Davis, Webb}.

Outline

- 1 Some results about $\binom{m}{n}$ during the late 1800
- 2 Some recent works for a prime power modulus
- 3 Our technique
- 4 Catalan numbers modulus 2^k
- 5 Catalan numbers modulus an odd prime power

The n -th Catalan number is defined as $c_n = \frac{1}{n+1} \binom{2n}{n}$.

The n -th Catalan number is defined as $c_n = \frac{1}{n+1} \binom{2n}{n}$.

Theorem (Deutsch and Sagan, 2006)

$$\omega_2(c_n) = d(n+1) - 1 = d(\alpha),$$

where $d(m) = m_0 + m_1 + \dots$ and

$$[n]_2 = \langle [\alpha]_2 \ 0 \ \underbrace{11 \dots 1}_2 \rangle_2.$$

This segment might be empty.

The n -th Catalan number is defined as $c_n = \frac{1}{n+1} \binom{2n}{n}$.

Theorem (Deutsch and Sagan, 2006)

$$\omega_2(c_n) = d(n+1) - 1 = d(\alpha),$$

where $d(m) = m_0 + m_1 + \dots$ and

$$[n]_2 = \langle [\alpha]_2 \ 0 \ \underbrace{11 \dots 1}_2 \rangle_2.$$

This segment might be empty.

- Postnikov and Sagan generalized this formula for a weighted Catalan number.

The n -th Catalan number is defined as $c_n = \frac{1}{n+1} \binom{2n}{n}$.

Theorem (Deutsch and Sagan, 2006)

$$\omega_2(c_n) = d(n+1) - 1 = d(\alpha),$$

where $d(m) = m_0 + m_1 + \dots$ and

$$[n]_2 = \langle [\alpha]_2 \ 0 \ \underbrace{11 \dots 1}_2 \rangle_2.$$

This segment might be empty.

- Postnikov and Sagan generalized this formula for a weighted Catalan number.
- A general formula of $\omega_p(c_n)$ for any prime p will be given later.

Let $d(n) = n_0 + n_1 + \cdots$ be the digit sum of $[n]_2$.

Let $d(n) = n_0 + n_1 + \cdots$ be the digit sum of $[n]_2$.

Proposition (Eu, Liu and Y.-N. Yeh, 2008)

First of all, $c_n \not\equiv_8 3, 7$ for any n . As for other congruences, we have

$$c_n \equiv_8 \begin{cases} \begin{matrix} 1 \\ 5 \\ 2 \\ 6 \end{matrix} & \text{if } d(\alpha) = 0 \text{ and } \begin{cases} \beta = 0 \text{ or } 1, \\ \beta \geq 2, \end{cases} \\ \begin{matrix} 4 \\ 0 \end{matrix} & \text{if } d(\alpha) = 1 \text{ and } \begin{cases} \alpha = 1, \\ \alpha \geq 2, \end{cases} \\ & \text{if } d(\alpha) = 2, \\ & \text{if } d(\alpha) \geq 3, \end{cases}$$

where $[n]_2 = \langle [\alpha]_2 \ 0 \ 1^\beta \rangle_2$.

Let $d(n) = n_0 + n_1 + \cdots$ be the digit sum of $[n]_2$.

Proposition (Eu, Liu and Y.-N. Yeh, 2008)

First of all, $c_n \not\equiv_8 3, 7$ for any n . As for other congruences, we have

$$c_n \equiv_8 \begin{cases} \begin{matrix} 1 \\ 5 \\ 2 \\ 6 \end{matrix} & \text{if } d(\alpha) = 0 \text{ and } \begin{cases} \beta = 0 \text{ or } 1, \\ \beta \geq 2, \end{cases} \\ \begin{matrix} 4 \\ 0 \end{matrix} & \text{if } d(\alpha) = 1 \text{ and } \begin{cases} \alpha = 1, \\ \alpha \geq 2, \end{cases} \\ & \text{if } d(\alpha) = 2, \\ & \text{if } d(\alpha) \geq 3, \end{cases}$$

where $[n]_2 = \langle [\alpha]_2 \ 0 \ 1^\beta \rangle_2$.

- e.g. $[83]_2 = \langle 1010011 \rangle_2$ has $[\alpha]_2 = \langle 1010 \rangle_2$, $d(\alpha) = 2$ and $\beta = 2$.

Let $d(n) = n_0 + n_1 + \cdots$ be the digit sum of $[n]_2$.

Proposition (Eu, Liu and Y.-N. Yeh, 2008)

First of all, $c_n \not\equiv_8 3, 7$ for any n . As for other congruences, we have

$$c_n \equiv_8 \begin{cases} \begin{matrix} 1 \\ 5 \\ 2 \\ 6 \end{matrix} & \text{if } d(\alpha) = 0 \text{ and } \begin{cases} \beta = 0 \text{ or } 1, \\ \beta \geq 2, \end{cases} \\ \begin{matrix} 4 \\ 0 \end{matrix} & \text{if } d(\alpha) = 1 \text{ and } \begin{cases} \alpha = 1, \\ \alpha \geq 2, \end{cases} \\ & \text{if } d(\alpha) = 2, \\ & \text{if } d(\alpha) \geq 3, \end{cases}$$

where $[n]_2 = \langle [\alpha]_2 \ 0 \ 1^\beta \rangle_2$.

- e.g. $[83]_2 = \langle 1010011 \rangle_2$ has $[\alpha]_2 = \langle 1010 \rangle_2$, $d(\alpha) = 2$ and $\beta = 2$.
- Therefore, $c_{83} \equiv_8 4$.

The Motzkin number can be defined as $M_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} c_k$.

Proposition (Eu, Liu and Y.-N. Yeh, 2008)

We have $M_n \equiv_4 0$ if and only if

$$n = (4i + 1)4^{j+1} - 1 \quad \text{or} \quad n = (4i + 3)4^{j+1} - 2,$$

and $M_n \equiv_4 2$ if and only if

$$n = (4i + 1)4^{j+1} - 2 \quad \text{or} \quad n = (4i + 3)4^{j+1} - 1,$$

where $i, j \in \mathbb{N}$.

Proposition (Eu, Liu and Y.-N. Yeh, 2008)

The Motzkin number M_n is even if and only if $n = (4i + \varepsilon)4^{j+1} - \delta$ for $i, j \in \mathbb{N}$, $\varepsilon = 1, 3$ and $\delta = 1, 2$. And we never have $M_n \equiv_8 0$. Precisely, we have

$$M_n \equiv_8 \begin{cases} 4 & \text{if } (\varepsilon, \delta) = (1, 1) \text{ or } (3, 2); \\ 4y + 2 & \text{if } (\varepsilon, \delta) = (1, 2) \text{ or } (3, 1), \end{cases}$$

where y is the number of digit 1's in $[4i + \varepsilon - 1]_2$.

Outline

- 1 Some results about $\binom{m}{n}$ during the late 1800
- 2 Some recent works for a prime power modulus
- 3 Our technique**
- 4 Catalan numbers modulus 2^k
- 5 Catalan numbers modulus an odd prime power

Main idea I: ω_p , CF_p and $E_{q,t}$

- **Problem 1:** To evaluate congruence for the combinatorial numbers of form $\frac{\prod_{i=1}^h M_i}{\prod_{j=1}^g N_j} \pmod{q := p^k}$.
- Problem 2:** To classify these combinatorial numbers \pmod{q} according to their congruences.

Main idea I: ω_p , CF_p and $E_{q,t}$

- **Problem 1:** To evaluate congruence for the combinatorial numbers of form $\frac{\prod_{i=1}^h M_i}{\prod_{j=1}^g N_j} \pmod{q := p^k}$.
- **Problem 2:** To classify these combinatorial numbers \pmod{q} according to their congruences.
- $CF_p(n) := \frac{n}{p^{\omega_p(n)}}$, the *cofactor* of n with respect to $p^{\omega_p(n)}$ (or *non- p -cofactor*).

Main idea I: ω_p , CF_p and $E_{q,t}$

- **Problem 1:** To evaluate congruence for the combinatorial numbers of form $\frac{\prod_{i=1}^h M_i}{\prod_{j=1}^g N_j} \pmod{q := p^k}$.
- **Problem 2:** To classify these combinatorial numbers \pmod{q} according to their congruences.
- $CF_p(n) := \frac{n}{p^{\omega_p(n)}}$, the *cofactor* of n with respect to $p^{\omega_p(n)}$ (or *non- p -cofactor*).
- To evaluate a product $M := \prod_{i=1}^h M_i$ modulo $q = p^k$, let us consider two cofactors of M , namely

$$p^{\omega_p(M)} = p^{\sum_{i=1}^h \omega_p(M_i)} \quad \text{and}$$

$$CF_p(M) = \prod_{i=1}^h CF_p(M_i).$$

Main idea I: ω_p , CF_p and $E_{q,t}$

- We analyze further that

$$\prod_{i=1}^h CF_p(M_i) \equiv_q \prod_{t \in \mathbb{Z}_q^*} t^{E_{q,t}(M)},$$

where $\mathbb{Z}_q^* = \{1, 2, \dots, q-1\} - \{mp \mid m \in \mathbb{N}\}$ and $E_{q,t}(M) := \sum_{i=1}^h \chi(CF_p(M_i) \equiv_q t)$.

Main idea I: ω_p , CF_p and $E_{q,t}$

- We analyze further that

$$\prod_{i=1}^h CF_p(M_i) \equiv_q \prod_{t \in \mathbb{Z}_q^*} t^{E_{q,t}(M)},$$

where $\mathbb{Z}_q^* = \{1, 2, \dots, q-1\} - \{mp \mid m \in \mathbb{N}\}$ and

$$E_{q,t}(M) := \sum_{i=1}^h \chi(CF_p(M_i) \equiv_q t).$$

- We call $E_{q,t}(M)$ the *t-encounter function of modulus q* w.r.t. the product $M := \prod_{i=1}^h M_i$.

Main idea I: ω_p , CF_p and $E_{q,t}$

- If $\omega_p(\prod_{i=1}^h M_i) \geq k$, then $\prod_{i=1}^h M_i \equiv_q 0$; otherwise

$$\prod_{i=1}^h M_i \equiv_q p^{\omega_p(\prod_{i=1}^h M_i)} \prod_{t \in \mathbb{Z}_q^*} t^{E_{q,t}(\prod_{i=1}^h M_i)}.$$

Main idea I: ω_p , CF_p and $E_{q,t}$

- If $\omega_p(\prod_{i=1}^h M_i) \geq k$, then $\prod_{i=1}^h M_i \equiv_q 0$; otherwise

$$\prod_{i=1}^h M_i \equiv_q p^{\omega_p(\prod_{i=1}^h M_i)} \prod_{t \in \mathbb{Z}_q^*} t^{E_{q,t}(\prod_{i=1}^h M_i)}.$$

- The idea can easily apply to $\frac{\prod_{i=1}^h M_i}{\prod_{j=1}^g N_j}$, if this fraction is actually an integer.

Main idea I: ω_p , CF_p and $E_{q,t}$

- If $\omega_p(\prod_{i=1}^h M_i) \geq k$, then $\prod_{i=1}^h M_i \equiv_q 0$; otherwise

$$\prod_{i=1}^h M_i \equiv_q p^{\omega_p(\prod_{i=1}^h M_i)} \prod_{t \in \mathbb{Z}_q^*} t^{E_{q,t}(\prod_{i=1}^h M_i)}.$$

- The idea can easily apply to $\frac{\prod_{i=1}^h M_i}{\prod_{j=1}^g N_j}$, if this fraction is actually an integer.
- Since $c_n = \frac{1}{n+1} \binom{2n}{n}$, we have

$$\begin{aligned} c_n &\equiv_q p^{-\omega_p(n+1) + \omega_p((2n)!) - 2\omega_p(n!)} \\ &\quad \times \frac{1}{CF_p(n+1)} \prod_{t \in \mathbb{Z}_q^*} t^{E_{q,t}((2n)!) - 2E_{q,t}(n!)}. \end{aligned}$$

Main idea II

- Let $q = p^k$. We have a bijection T_q as follows

$$T_q : (\mathbb{Z}_{2^k}^*, \times_q) \rightarrow (C_2 \times C_{2^{k-2}}, +) \quad \text{for } k \geq 2;$$

$$T_q : (\mathbb{Z}_{p^k}^*, \times_q) \rightarrow (C_{p^{k-1}(p-1)}, +) \quad \text{for an odd prime } p.$$

Main idea II

- Let $q = p^k$. We have a bijection T_q as follows

$$T_q : (\mathbb{Z}_{2^k}^*, \times_q) \rightarrow (C_2 \times C_{2^{k-2}}, +) \quad \text{for } k \geq 2;$$

$$T_q : (\mathbb{Z}_{p^k}^*, \times_q) \rightarrow (C_{p^{k-1}(p-1)}, +) \quad \text{for an odd prime } p.$$

- Let $A = C_2 \times C_{2^{k-2}}$ or $A = C_{p^{k-1}(p-1)}$. If we want to use A , then we need to consider

$$CF_p\left(\prod_{i=1}^h M_i\right) \equiv_q T_q^{-1} \left(\sum_{t \in \mathbb{Z}_q^*} T_q(t) E_{q,t} \left(\prod_{i=1}^h M_i \right) \right) \text{ or}$$

$$T_q \left(CF_p\left(\prod_{i=1}^h M_i\right) \pmod{q} \right) \equiv_A \sum_{y \in A} y E_{q,T^{-1}(y)} \left(\prod_{i=1}^h M_i \right).$$

Main idea II

- Let $q = p^k$. We have a bijection T_q as follows

$$T_q : (\mathbb{Z}_{2^k}^*, \times_q) \rightarrow (C_2 \times C_{2^{k-2}}, +) \quad \text{for } k \geq 2;$$

$$T_q : (\mathbb{Z}_{p^k}^*, \times_q) \rightarrow (C_{p^{k-1}(p-1)}, +) \quad \text{for an odd prime } p.$$

- Let $A = C_2 \times C_{2^{k-2}}$ or $A = C_{p^{k-1}(p-1)}$. If we want to use A , then we need to consider

$$CF_p\left(\prod_{i=1}^h M_i\right) \equiv_q T_q^{-1} \left(\sum_{t \in \mathbb{Z}_q^*} T_q(t) E_{q,t} \left(\prod_{i=1}^h M_i \right) \right) \text{ or}$$

$$T_q \left(CF_p\left(\prod_{i=1}^h M_i\right) \right) \equiv_A \sum_{y \in A} y E_{q,T^{-1}(y)} \left(\prod_{i=1}^h M_i \right).$$

Recall that $d(n) = n_0 + n_1 + \dots$, where $[n]_p = \langle \dots n_1 n_0 \rangle_p$.

Define $d_k(n) = n_k + n_{k+1} + \dots$.

Lemma

Let $q = p^k$, $t \in \mathbb{Z}_q^*$ and $[n]_p = \langle n_r n_{r-1} \dots n_1 n_0 \rangle_p$. We have

$$\begin{aligned} \omega_p(n!) &= \frac{n - d(n)}{p - 1}, \\ E_{q,t}(n!) &= \frac{|\langle n_r \dots n_{k-1} \rangle_p| - d_{k-1}(n)}{p - 1}, \\ &+ \sum_{i \geq 0} \chi(|\langle n_{i+k-1} \dots n_{i+1} n_i \rangle_p| \geq t). \end{aligned}$$

Recall that $d(n) = n_0 + n_1 + \dots$, where $[n]_p = \langle \dots n_1 n_0 \rangle_p$.

Define $d_k(n) = n_k + n_{k+1} + \dots$.

Lemma

Let $q = p^k$, $t \in \mathbb{Z}_q^*$ and $[n]_p = \langle n_r n_{r-1} \dots n_1 n_0 \rangle_p$. We have

$$\omega_p(n!) = \frac{n - d(n)}{p - 1},$$

$$E'_q(n!) = \frac{|\langle n_r \dots n_{k-1} \rangle_p| - d_{k-1}(n)}{p - 1},$$

$$E''_{q,t}(n!) = \sum_{i \geq 0} \chi(|\langle n_{i+k-1} \dots n_{i+1} n_i \rangle_p| \geq t).$$

Recall that $d(n) = n_0 + n_1 + \dots$, where $[n]_p = \langle \dots n_1 n_0 \rangle_p$.

Define $d_k(n) = n_k + n_{k+1} + \dots$.

Lemma

Let $q = p^k$, $t \in \mathbb{Z}_q^*$ and $[n]_p = \langle n_r n_{r-1} \dots n_1 n_0 \rangle_p$. We have

$$\omega_p(n!) = \frac{n - d(n)}{p - 1},$$

$$E'_q(n!) = \frac{|\langle n_r \dots n_{k-1} \rangle_p| - d_{k-1}(n)}{p - 1},$$

$$E''_{q,t}(n!) = \sum_{i \geq 0} \chi(|\langle n_{i+k-1} \dots n_{i+1} n_i \rangle_p| \geq t).$$

where $\mathcal{S}(n) = \{|\langle n_{k+i-1} \dots n_{i+1} n_i \rangle_p| : \text{except } 0\}_{i \geq 0}$ is a multi-set and $\#(\mathcal{S}, T)$ is the number of elements (with multiplicity) in \mathcal{S} belonging to T .

Recall that $d(n) = n_0 + n_1 + \dots$, where $[n]_p = \langle \dots n_1 n_0 \rangle_p$.

Define $d_k(n) = n_k + n_{k+1} + \dots$.

Lemma

Let $q = p^k$, $t \in \mathbb{Z}_q^*$ and $[n]_p = \langle n_r n_{r-1} \dots n_1 n_0 \rangle_p$. We have

$$\omega_p(n!) = \frac{n - d(n)}{p - 1},$$

$$E'_q(n!) = \frac{|\langle n_r \dots n_{k-1} \rangle_p| - d_{k-1}(n)}{p - 1},$$

$$E''_{q,t}(n!) = \#(\mathcal{S}(n), [t, q - 1]).$$

where $\mathcal{S}(n) = \{|\langle n_{k+i-1} \dots n_{i+1} n_i \rangle_p| : \text{except } 0\}_{i \geq 0}$ is a multi-set and $\#(\mathcal{S}, T)$ is the number of elements (with multiplicity) in \mathcal{S} belonging to T .

■ Therefore, $CF_p(n!) \equiv_q \left(\prod_{t \in \mathbb{Z}_q^*} t \right)^{E'_q(n!)} \times \prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}(n!)}.$

- Therefore, $CF_p(n!) \equiv_q \left(\prod_{t \in \mathbb{Z}_q^*} t \right)^{E'_q(n!)} \times \prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}(n!)}.$
- For $p = 2$ and $k \geq 3$, we have

$$\sum_{y \in C_2 \times C_{2^k-2}} y \equiv (0,0); \text{ equivalently, } \prod_{t \in \mathbb{Z}_{2^k}^*} t \equiv_q 1;$$

So $E'_q(n!)$ is useless for evaluating $CF_p(n!) \pmod{2^k}$.

- Therefore, $CF_p(n!) \equiv_q \left(\prod_{t \in \mathbb{Z}_q^*} t \right)^{E'_q(n!)} \times \prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}(n!)}.$
- For $p = 2$ and $k \geq 3$, we have

$$\sum_{y \in C_2 \times C_{2^{k-2}}} y \equiv (0, 0); \text{ equivalently, } \prod_{t \in \mathbb{Z}_{2^k}^*} t \equiv_q 1;$$

So $E'_q(n!)$ is useless for evaluating $CF_p(n!) \pmod{2^k}$.

- For an odd prime p , we have

$$\sum_{y \in C_{p^{k-1}(p-1)}} y \equiv p^{k-1}(p-1)/2; \text{ equivalently, } \prod_{t \in \mathbb{Z}_{p^k}^*} t \equiv_q -1.$$

We only care about the parity of $E'_q(n!)$.

Outline

- 1 Some results about $\binom{m}{n}$ during the late 1800
- 2 Some recent works for a prime power modulus
- 3 Our technique
- 4 Catalan numbers modulus 2^k
- 5 Catalan numbers modulus an odd prime power

- We use the bijection $T_q : \mathbb{Z}_{2^k}^* \rightarrow C_2 \times C_{q/4}$ to study $c_n \pmod{2^k}$. Define $T_q(t) := (b(t), u_q(t))$.

- We use the bijection $T_q : \mathbb{Z}_{2^k}^* \rightarrow C_2 \times C_{q/4}$ to study $c_n \pmod{2^k}$. Define $T_q(t) := (b(t), u_q(t))$.
- $$b(t) = \begin{cases} 0 & \text{if } t \equiv_4 1; \\ 1 & \text{if } t \equiv_4 3. \end{cases}$$

- We use the bijection $T_q : \mathbb{Z}_{2^k}^* \rightarrow C_2 \times C_{q/4}$ to study $c_n \pmod{2^k}$. Define $T_q(t) := (b(t), u_q(t))$.
- $$b(t) = \begin{cases} 0 & \text{if } t \equiv_4 1; \\ 1 & \text{if } t \equiv_4 3. \end{cases}$$
- $b(CF_2(n!)) \equiv_2 r(n) + n_0 + n_1 \equiv_2 zr(n) + n_1$,
where $r(n)$ is the number of runs of 1 in $[n]_2$ and $zr(n)$ is the number of runs of 0.

- We use the bijection $T_q : \mathbb{Z}_{2^k}^* \rightarrow C_2 \times C_{q/4}$ to study $c_n \pmod{2^k}$. Define $T_q(t) := (b(t), u_q(t))$.
- $$b(t) = \begin{cases} 0 & \text{if } t \equiv_4 1; \\ 1 & \text{if } t \equiv_4 3. \end{cases}$$
- $b(CF_2(n!)) \equiv_2 r(n) + n_0 + n_1 \equiv_2 zr(n) + n_1$,
where $r(n)$ is the number of runs of 1 in $[n]_2$ and $zr(n)$ is the number of runs of 0.
- $$\begin{aligned} u_q(CF_2(n!)) &\equiv_{q/4} \sum_{\substack{3 \leq t \leq s \leq q-1 \\ t: \text{ odd}}} \#(\mathcal{S}(n), \{s\}) u_q(t) \\ &= \sum_{s \in [3, q-2]} \#(\mathcal{S}(n), \{s\}) \sum_{t \in [3, s]_{\text{odd}}} u_q(t). \end{aligned}$$

- We use the bijection $T_q : \mathbb{Z}_{2^k}^* \rightarrow C_2 \times C_{q/4}$ to study $c_n \pmod{2^k}$. Define $T_q(t) := (b(t), u_q(t))$.
- $$b(t) = \begin{cases} 0 & \text{if } t \equiv_4 1; \\ 1 & \text{if } t \equiv_4 3. \end{cases}$$
- $b(CF_2(n!)) \equiv_2 r(n) + n_0 + n_1 \equiv_2 zr(n) + n_1$,
where $r(n)$ is the number of runs of 1 in $[n]_2$ and $zr(n)$ is the number of runs of 0.
- $$\begin{aligned} u_q(CF_2(n!)) &\equiv_{q/4} \sum_{\substack{3 \leq t \leq s \leq q-1 \\ t: \text{ odd}}} \#(\mathcal{S}(n), \{s\}) u_q(t) \\ &= \sum_{s \in [3, q-2]} \#(\mathcal{S}(n), \{s\}) \sum_{t \in [3, s]_{\text{odd}}} u_q(t). \end{aligned}$$
- We built a table for $\sum_{t \in [3, s]_{\text{odd}}} u_q(t)$ or $\prod_{t \in [3, s]_{\text{odd}}} t$ according to $s \in [3, q-2]$ to study $c_n \pmod{16}$ and $c_n \pmod{64}$.

Lemma

Let m be an integer such that $[m]_2$ is obtained by either extending or truncating some runs of 0 or 1 of length $\geq k-1$ in $[n]_2$ to be different length but still $\geq k-1$. We have

$$b(CF_2(n!)) = b(CF_2(m!)) \text{ and } u_q(CF_2(n!)) = u_q(CF_2(m!)),$$

and then

$$CF_2(n!) \equiv_q CF_2(m!).$$

Lemma

Let m be an integer such that $[m]_2$ is obtained by either extending or truncating some runs of 0 or 1 of length $\geq k - 1$ in $[n]_2$ to be different length but still $\geq k - 1$. We have

$$b(CF_2(n!)) = b(CF_2(m!)) \text{ and } u_q(CF_2(n!)) = u_q(CF_2(m!)),$$

and then

$$CF_2(n!) \equiv_q CF_2(m!).$$

Pf. $b(CF_2(n!)) \equiv_2 zr(n) + n_1 \equiv_2 zr(m) + m_1 \equiv_2 b(CF_2(m!)).$

Lemma

Let m be an integer such that $[m]_2$ is obtained by either extending or truncating some runs of 0 or 1 of length $\geq k-1$ in $[n]_2$ to be different length but still $\geq k-1$. We have

$$b(CF_2(n!)) = b(CF_2(m!)) \text{ and } u_q(CF_2(n!)) = u_q(CF_2(m!)),$$

and then

$$CF_2(n!) \equiv_q CF_2(m!).$$

Pf. $b(CF_2(n!)) \equiv_2 zr(n) + n_1 \equiv_2 zr(m) + m_1 \equiv_2 b(CF_2(m!)).$

$$u_q(CF_2(n!)) \equiv_{q/4} \sum_{s \in [3, q-3]_{\text{odd}}} \#(\mathcal{S}(n), \{s, s+1\}) \sum_{t \in [3, s]_{\text{odd}}} u_q(t)$$

is independent on the numbers of $\langle 0^{k-1} \rangle_2$ and $\langle 1^{k-1} \rangle_2$ in $[n]_2$.

Given $n \in \mathbb{N}$, let \bar{n} be the integer such that $[\bar{n}]_2$ is obtained by the following rules.

- a. When the rightmost run of 0 in $[n]_2$ is of length $\geq k+1$, let us truncate it to be length k , otherwise keep it the same.

Given $n \in \mathbb{N}$, let \bar{n} be the integer such that $[\bar{n}]_2$ is obtained by the following rules.

- When the rightmost run of 0 in $[n]_2$ is of length $\geq k+1$, let us truncate it to be length k , otherwise keep it the same.
- For any other run of 0 or 1 of $[n]_2$ with length $\geq k$, truncate them to be length $k-1$.

Theorem (Liu and Yeh, 2010)

Let $n, k \in \mathbb{N}$ with $k \geq 3$. We have

$$c_n \equiv_{2^k} \begin{cases} c_{\bar{n}} & \text{for } d(\alpha) \leq k-1, \text{ and} \\ 0 & \text{for } d(\alpha) \geq k. \end{cases}$$

Given $n \in \mathbb{N}$, let \bar{n} be the integer such that $[\bar{n}]_2$ is obtained by the following rules.

- When the rightmost run of 0 in $[n]_2$ is of length $\geq k+1$, let us truncate it to be length k , otherwise keep it the same.
- For any other run of 0 or 1 of $[n]_2$ with length $\geq k$, truncate them to be length $k-1$.

Theorem (Liu and Yeh, 2010)

Let $n, k \in \mathbb{N}$ with $k \geq 3$. We have

$$c_n \equiv_{2^k} \begin{cases} c_{\bar{n}} & \text{for } d(\alpha) \leq k-1, \text{ and} \\ 0 & \text{for } d(\alpha) \geq k. \end{cases}$$

Example. $c_{\langle 100001111 \rangle_2} \equiv_8 6, \quad c_{\langle 1111111 \rangle_2} \equiv_{16} 13,$
 $c_{\langle 100011 \rangle_2} \equiv_8 6, \quad c_{\langle 111 \rangle_2} \equiv_{16} 13.$

Theorem (Liu and Yeh, 2010)

Let $n \in \mathbb{N}$ and $q = 2^k$ with $k \geq 2$. Then we have

$$c_n \equiv_q (-1)^{zr(\alpha)} 2^{d(\alpha)} 5^{u_q(CF_2(c_n))}.$$

In particular, when $k = 2$ we have

$$c_n \equiv_4 (-1)^{zr(\alpha)} 2^{d(\alpha)}.$$

Proposition (Liu and Yeh, 2010)

Let c_n be the n -th Catalan number. First of all, $c_n \not\equiv_{16} 3, 7, 9, 11, 15$ for any n . As for the other congruences, we have

$$c_n \equiv_{16} \begin{cases} \begin{matrix} 1 \\ 5 \\ 13 \end{matrix} & \text{if } d(\alpha) = 0 \text{ and } \begin{cases} \beta \leq 1, \\ \beta = 2, \\ \beta \geq 3, \end{cases} \\ \begin{matrix} 2 \\ 10 \end{matrix} & \text{if } d(\alpha) = 1, \alpha = 1 \text{ and } \begin{cases} \beta = 0 \text{ or } \beta \geq 2, \\ \beta = 1, \end{cases} \\ \begin{matrix} 6 \\ 14 \end{matrix} & \text{if } d(\alpha) = 1, \alpha \geq 2 \text{ and } \begin{cases} (\alpha = 2, \beta \geq 2) \text{ or } (\alpha \geq 3, \beta \leq 1), \\ (\alpha = 2, \beta \leq 1) \text{ or } (\alpha \geq 3, \beta \geq 2), \end{cases} \\ \begin{matrix} 4 \\ 12 \end{matrix} & \text{if } d(\alpha) = 2 \text{ and } \begin{cases} zr(\alpha) \neq 1, \\ zr(\alpha) = 1, \end{cases} \\ 8 & \text{if } d(\alpha) = 3, \\ 0 & \text{if } d(\alpha) \geq 4. \end{cases}$$

where $[n]_2 = \langle [\alpha]_2 \ 0 \ 1^\beta \rangle_2$.

We also completely classified $c_n \pmod{64}$. Here we only post the classification for odd congruences.

Proposition (Liu and Yeh, 2010)

Let $n \in \mathbb{N}$ with $d(\alpha) = 0$, i.e. $n = 2^\beta - 1$. Then we have

$$c_n \equiv_{64} \begin{cases} 1 & \text{if } \beta = 0 \text{ or } 1; \\ 5 & \text{if } \beta = 2; \\ 45 & \text{if } \beta = 3; \\ 61 & \text{if } \beta = 4; \\ 29 & \text{if } \beta \geq 5. \end{cases}$$

Moreover, any number in $[1, 63]_{\text{odd}} - \{1, 5, 29, 45, 61\}$ can never be the congruence of $c_n \pmod{64}$.

After observing all odd congruences from modulus 4 up to modulus 1024, once we conjectured the following property. This property was proved recently.

Theorem (Lin, 2010)

Let $k \geq 2$. Only $k - 1$ different odd congruences $c_n \pmod{2^k}$ exist, and they are

$$c_{2^m-1} \pmod{2^k}$$

for $m = 1, 2, \dots, k - 1$.

After observing all odd congruences from modulus 4 up to modulus 1024, once we conjectured the following property. This property was proved recently.

Theorem (Lin, 2010)

Let $k \geq 2$. Only $k - 1$ different odd congruences $c_n \pmod{2^k}$ exist, and they are

$$c_{2^m-1} \pmod{2^k}$$

for $m = 1, 2, \dots, k - 1$.

Example There are only 6 congruences $c_n \pmod{128}$ with odd value:

$$\begin{array}{ll} c_{\langle 1 \rangle_2} \equiv_{128} 1, & c_{\langle 11 \rangle_2} \equiv_{128} 5, \\ c_{\langle 111 \rangle_2} \equiv_{128} 45, & c_{\langle 1111 \rangle_2} \equiv_{128} 125, \\ c_{\langle 11111 \rangle_2} \equiv_{128} 29, & c_{\langle 111111 \rangle_2} \equiv_{128} 93. \end{array}$$

Outline

- 1 Some results about $\binom{m}{n}$ during the late 1800
- 2 Some recent works for a prime power modulus
- 3 Our technique
- 4 Catalan numbers modulus 2^k
- 5 Catalan numbers modulus an odd prime power

- Let $\kappa_p(m, n; i) := \left\lfloor \frac{|\langle m_i \dots m_0 \rangle_p| + |\langle n_i \dots n_0 \rangle_p|}{p^{i+1}} \right\rfloor$ ($= 0$ or 1) be the possible *carry* from the i -th to the $(i + 1)$ -st places for $m + n$ in the base- p system.

- Let $\kappa_p(m, n; i) := \left\lfloor \frac{|\langle m_i \dots m_0 \rangle_p| + |\langle n_i \dots n_0 \rangle_p|}{p^{i+1}} \right\rfloor$ ($= 0$ or 1) be the possible *carry* from the i -th to the $(i + 1)$ -st places for $m + n$ in the base- p system.
- Let $C_p(m, n; i) := \sum_{j \geq i} \kappa_p(m, n; j)$ and $C_p(m, n) = C_p(m, n; 0)$ which is the number of total carries.

- Let $\kappa_p(m, n; i) := \left\lfloor \frac{|\langle m_i \dots m_0 \rangle_p| + |\langle n_i \dots n_0 \rangle_p|}{p^{i+1}} \right\rfloor$ ($= 0$ or 1) be the possible *carry* from the i -th to the $(i+1)$ -st places for $m+n$ in the base- p system.
- Let $C_p(m, n; i) := \sum_{j \geq i} \kappa_p(m, n; j)$ and $C_p(m, n) = C_p(m, n; 0)$ which is the number of total carries.
- $d(m+n) = d(m) + d(n) - (p-1)C_p(m, n);$
 $\omega_p((m+n)!) = \frac{m+n-d(m)-d(n)}{p-1} + C_p(m, n).$

- Let $\kappa_p(m, n; i) := \left\lfloor \frac{|\langle m_i \dots m_0 \rangle_p| + |\langle n_i \dots n_0 \rangle_p|}{p^{i+1}} \right\rfloor$ ($= 0$ or 1) be the possible *carry* from the i -th to the $(i+1)$ -st places for $m+n$ in the base- p system.
- Let $C_p(m, n; i) := \sum_{j \geq i} \kappa_p(m, n; j)$ and $C_p(m, n) = C_p(m, n; 0)$ which is the number of total carries.
- $d(m+n) = d(m) + d(n) - (p-1)C_p(m, n);$
 $\omega_p((m+n)!) = \frac{m+n-d(m)-d(n)}{p-1} + C_p(m, n).$

Theorem

We have

$$\omega_p(c_n) = C_p(n, n) - \beta = C_p(n, n; \beta),$$

where $[n]_p = \langle \dots \widetilde{(p-1)} (p-1)^\beta \rangle_p$.

- Let $\kappa_p(m, n; i) := \left\lfloor \frac{|\langle m_i \dots m_0 \rangle_p| + |\langle n_i \dots n_0 \rangle_p|}{p^{i+1}} \right\rfloor$ ($= 0$ or 1) be the possible *carry* from the i -th to the $(i+1)$ -st places for $m+n$ in the base- p system.
- Let $C_p(m, n; i) := \sum_{j \geq i} \kappa_p(m, n; j)$ and $C_p(m, n) = C_p(m, n; 0)$ which is the number of total carries.
- $d(m+n) = d(m) + d(n) - (p-1)C_p(m, n);$
 $\omega_p((m+n)!) = \frac{m+n-d(m)-d(n)}{p-1} + C_p(m, n).$

Theorem

We have

$$\omega_p(c_n) = C_p(n, n) - \beta = C_p(n, n; \beta),$$

where $[n]_p = \langle \dots \widetilde{(p-1)} (p-1)^\beta \rangle_p$.

If $p = 2$, then $C_2(n, n; \beta) = d(\alpha)$, where $[n]_2 = \langle [\alpha]_2 \ 0 \ 1^\beta \rangle_2$.

\Rightarrow Theorem of Deutsch and Sagan.

Let \oplus_q be the operator of addition over ring \mathbb{Z}_q , and

$z(m, n; i) = |\langle m_{i+k-1} \dots m_i \rangle_p| \oplus_q |\langle n_{i+k-1} \dots n_i \rangle_p|$. Then

$$\langle (m+n)_{i+k-1} \dots (m+n)_i \rangle_p = [z(m, n; i) \oplus_q \kappa(m, n; i-1)]_p.$$

Let \oplus_q be the operator of addition over ring \mathbb{Z}_q , and

$z(m, n; i) = |\langle m_{i+k-1} \dots m_i \rangle_p| \oplus_q |\langle n_{i+k-1} \dots n_i \rangle_p|$. Then

$$\langle (m+n)_{i+k-1} \dots (m+n)_i \rangle_p = [z(m, n; i) \oplus_q \kappa(m, n; i-1)]_p.$$

Lemma (From now on p is an odd prime.)

$$\begin{aligned} E'_q((m+n)!) &= \frac{|\langle \dots m_{k-1} \rangle_p| + |\langle \dots n_{k-1} \rangle_p| - d_{k-1}(m) - d_{k-1}(n)}{p-1} \\ &\quad + C(m, n; k-1); \\ E''_{q,t}((m+n)!) &= \sum_{i \geq 0} \left[\begin{array}{c} \chi(z(m, n; i) \geq t) \\ + \chi(z(m, n; i) = t-1) \kappa(m, n; i-1) \end{array} \right] \\ &\quad - \sigma(m, n), \end{aligned}$$

where $\sigma(m, n)$ be # of i st. $z(m, n; i) = q-1$ and $\kappa(m, n; i-1) = 1$.

because $\sigma(m, n)$ is independent on t , let's modify E'_q and $E''_{q,t}$.

Let \oplus_q be the operator of addition over ring \mathbb{Z}_q , and

$z(m, n; i) = |\langle m_{i+k-1} \dots m_i \rangle_p| \oplus_q |\langle n_{i+k-1} \dots n_i \rangle_p|$. Then

$$\langle (m+n)_{i+k-1} \dots (m+n)_i \rangle_p = [z(m, n; i) \oplus_q \kappa(m, n; i-1)]_p.$$

Lemma (From now on p is an odd prime.)

$$\begin{aligned} E'_q((m+n)!) &= \frac{|\langle \dots m_{k-1} \rangle_p| + |\langle \dots n_{k-1} \rangle_p| - d_{k-1}(m) - d_{k-1}(n)}{p-1} \\ &\quad + C(m, n; k-1) - \sigma(m, n); \\ E''_{q,t}((m+n)!) &= \sum_{i \geq 0} \left[\begin{array}{c} \chi(z(m, n; i) \geq t) \\ + \chi(z(m, n; i) = t-1) \kappa(m, n; i-1) \end{array} \right] \end{aligned}$$

Because $\sigma(m, n)$ is independent on t , let's modify E'_q and $E''_{q,t}$.

Let \oplus_q be the operator of addition over ring \mathbb{Z}_q , and

$z(m, n; i) = |\langle m_{i+k-1} \dots m_i \rangle p| \oplus_q |\langle n_{i+k-1} \dots n_i \rangle p|$. Then

$$\langle (m+n)_{i+k-1} \dots (m+n)_i \rangle p = [z(m, n; i) \oplus_q \kappa(m, n; i-1)]_p.$$

Lemma (final version)

$$E'_q((m+n)!) \equiv_2 \sum_{j \geq 0} (m_{2j+k} + n_{2j+k}) + C(m, n; k-1) - \sigma(m, n);$$

$$E''_{q,t}((m+n)!) = \#(\mathcal{S}^+, [t, q-1]) + \#(\bar{\mathcal{S}}^+, \{t-1\}),$$

where $\mathcal{S}^+ = \{z(m, n; i) : z(m, n; i) \neq 0\}_{i \geq 0}$,

$\bar{\mathcal{S}}^+ = \{z \in \mathcal{S}^+ : \kappa(m, n; i-1) = 1 \text{ and } z_0 \neq p-1\}$, and

$\sigma(m, n)$ is the number of i such that $z(m, n; i) = q-1$ and

$\kappa(m, n; i-1) = 1$

└ Catalan numbers modulus an odd prime power

└ $CF_q(c_n)$ for an odd prime power $q = p^k$

$$\blacksquare CF_q(c_n) \equiv_q \frac{1}{CF_q(n+1)} (-1)^{E'_q((n+n)!)-2E'_q(n!)} \\ \times \prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}((n+n)!)-2E''_{q,t}(n!)}.$$

└ Catalan numbers modulus an odd prime power

└ $CF_q(c_n)$ for an odd prime power $q = p^k$

- $CF_q(c_n) \equiv_q \frac{1}{CF_q(n+1)} (-1)^{E'_q((n+n)!)-2E'_q(n!)}$
 $\times \prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}((n+n)!)-2E''_{q,t}(n!)}.$
- Let $[n]_p = \langle \dots (p-1) (p-1)^\beta \rangle_p = \langle \dots n_\beta (p-1)^\beta \rangle_p$.
 So $[n+1]_p = \langle \dots n_{\beta+1} (n_\beta + 1) 0^\beta \rangle_p$ and then
 $CF_q(n+1) \equiv_q |\langle n_{\beta+k-1} \dots n_{\beta+1} (n_\beta + 1) \rangle_p|.$

└ Catalan numbers modulus an odd prime power

└ $CF_q(c_n)$ for an odd prime power $q = p^k$

- $CF_q(c_n) \equiv_q \frac{1}{CF_q(n+1)} (-1)^{E'_q((n+n)!)-2E'_q(n!)} \times \prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}((n+n)!)-2E''_{q,t}(n!)}.$
- Let $[n]_p = \langle \dots (p-1) (p-1)^\beta \rangle_p = \langle \dots n_\beta (p-1)^\beta \rangle_p$.
So $[n+1]_p = \langle \dots n_{\beta+1} (n_\beta + 1) 0^\beta \rangle_p$ and then
 $CF_q(n+1) \equiv_q |\langle n_{\beta+k-1} \dots n_{\beta+1} (n_\beta + 1) \rangle_p|.$
- $E'_q((n+n)!) \equiv_2 C_p(n, n; k-1) - \bar{\sigma}.$

where $\bar{\sigma} = |\{i : \langle n_{i+k-1} \dots n_i \rangle = \langle (\frac{p-1}{2})^{k-1} \rangle \text{ and } \kappa(n, n; i-1) = 1\}|.$

└ Catalan numbers modulus an odd prime power

└ $CF_q(c_n)$ for an odd prime power $q = p^k$

- $CF_q(c_n) \equiv_q \frac{1}{CF_q(n+1)} (-1)^{E'_q((n+n)!)-2E'_q(n!)}$
 $\times \prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}((n+n)!)-2E''_{q,t}(n!)}.$
- Let $[n]_p = \langle \dots (p-1) (p-1)^\beta \rangle_p = \langle \dots n_\beta (p-1)^\beta \rangle_p$.
 So $[n+1]_p = \langle \dots n_{\beta+1} (n_\beta + 1) 0^\beta \rangle_p$ and then
 $CF_q(n+1) \equiv_q |\langle n_{\beta+k-1} \dots n_{\beta+1} (n_\beta + 1) \rangle_p|.$
- $E'_q((n+n)!) \equiv_2 C_p(n, n; k-1) - \bar{\sigma}.$

where $\bar{\sigma} = |\{i : \langle n_{i+k-1} \dots n_i \rangle = \langle (\frac{p-1}{2})^{k-1} \rangle$
 and $\kappa(n, n; i-1) = 1\}|.$

However, once $\langle (\frac{p-1}{2})^{k-1} \rangle$ with $\kappa(n, n; i-1)$ appears in $[n]_p$,
 we have $C_p(n, n; \beta) \geq k$; and then $c_n \equiv_q 0$.

- $CF_q(c_n) \equiv_q \frac{1}{CF_q(n+1)} (-1)^{E'_q((n+n)!)-2E'_q(n!)} \times \prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}((n+n)!)-2E''_{q,t}(n!)}.$
- Let $[n]_p = \langle \dots (p-1) (p-1)^\beta \rangle_p = \langle \dots n_\beta (p-1)^\beta \rangle_p.$
So $[n+1]_p = \langle \dots n_{\beta+1} (n_\beta + 1) 0^\beta \rangle_p$ and then
 $CF_q(n+1) \equiv_q |\langle n_{\beta+k-1} \dots n_{\beta+1} (n_\beta + 1) \rangle_p|.$
- $E'_q((n+n)!) \equiv_2 C_p(n, n; k-1) - \bar{\sigma}.$

where $\bar{\sigma} = |\{i : \langle n_{i+k-1} \dots n_i \rangle = \langle (\frac{p-1}{2})^{k-1} \rangle \text{ and } \kappa(n, n; i-1) = 1\}|.$

However, once $\langle (\frac{p-1}{2})^{k-1} \rangle$ with $\kappa(n, n; i-1)$ appears in $[n]_p$, we have $C_p(n, n; \beta) \geq k$; and then $c_n \equiv_q 0$.

Therefore, $\bar{\sigma}$ is irrelevant for those $c_n \not\equiv_q 0$.

└ Catalan numbers modulus an odd prime power

└ $CF_q(c_n)$ for an odd prime power $q = p^k$

- $CF_q(c_n) \equiv_q \frac{1}{CF_q(n+1)} (-1)^{E'_q((n+n)!)-2E'_q(n!)} \times \prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}((n+n)!)-2E''_{q,t}(n!)}.$
- Let $[n]_p = \langle \dots \widetilde{(p-1)} (p-1)^\beta \rangle_p = \langle \dots n_\beta (p-1)^\beta \rangle_p$.
So $[n+1]_p = \langle \dots n_{\beta+1} (n_\beta + 1) 0^\beta \rangle_p$ and then
 $CF_q(n+1) \equiv_q |\langle n_{\beta+k-1} \dots n_{\beta+1} (n_\beta + 1) \rangle_p|.$
- $E'_q((n+n)!) \equiv_2 C_p(n, n; k-1) - \bar{\sigma}.$

- $CF_q(c_n) \equiv_q \frac{1}{CF_q(n+1)} (-1)^{E'_q((n+n)!)-2E'_q(n!)} \times \prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}((n+n)!)-2E''_{q,t}(n!)}.$
- Let $[n]_p = \langle \dots \widetilde{(p-1)} (p-1)^\beta \rangle_p = \langle \dots n_\beta (p-1)^\beta \rangle_p$.
So $[n+1]_p = \langle \dots n_{\beta+1} (n_\beta + 1) 0^\beta \rangle_p$ and then
 $CF_q(n+1) \equiv_q |\langle n_{\beta+k-1} \dots n_{\beta+1} (n_\beta + 1) \rangle_p|.$
- $E'_q((n+n)!) \equiv_2 C_p(n, n; k-1) - \bar{\sigma}.$
- By last lemma, we need $\mathcal{S}^+ = \{z(n, n; i) : z(n, n; i) \neq 0\}_{i \geq 0}$,
 $\bar{\mathcal{S}}^+ = \{z \in \mathcal{S}^+ : \kappa(n, n; i-1) = 1 \text{ and } z_0 \neq p-1\}$ and
 $\mathcal{S} := \{|\langle n_{k+i-1} \dots n_{i+1} n_i \rangle_p| \text{ except } 0\}_{i \geq 0}.$
Note that $\mathcal{S}^+ = \{2s \pmod q : s \in \mathcal{S}\}.$

- $CF_q(c_n) \equiv_q \frac{1}{CF_q(n+1)} (-1)^{E'_q((n+n)!)-2E'_q(n!)} \times \prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}((n+n)!)-2E''_{q,t}(n!)}.$
- Let $[n]_p = \langle \dots \widetilde{(p-1)} (p-1)^\beta \rangle_p = \langle \dots n_\beta (p-1)^\beta \rangle_p$.
So $[n+1]_p = \langle \dots n_{\beta+1} (n_\beta + 1) 0^\beta \rangle_p$ and then
 $CF_q(n+1) \equiv_q |\langle n_{\beta+k-1} \dots n_{\beta+1} (n_\beta + 1) \rangle_p|.$
- $E'_q((n+n)!) \equiv_2 C_p(n, n; k-1) - \bar{\sigma}.$
- By last lemma, we need $\mathcal{S}^+ = \{z(n, n; i) : z(n, n; i) \neq 0\}_{i \geq 0}$,
 $\bar{\mathcal{S}}^+ = \{z \in \mathcal{S}^+ : \kappa(n, n; i-1) = 1 \text{ and } z_0 \neq p-1\}$ and
 $\mathcal{S} := \{|\langle n_{k+i-1} \dots n_{i+1} n_i \rangle_p| \text{ except } 0\}_{i \geq 0}.$
Note that $\mathcal{S}^+ = \{2s \pmod{q} : s \in \mathcal{S}\}.$

To study $\prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}((n+n)!)-2E''_{q,t}(n!)}$, we need \mathcal{S}^+ , $\bar{\mathcal{S}}^+$ and \mathcal{S} .
But $\mathcal{S}^+ = 2\mathcal{S}$ and $\bar{\mathcal{S}}^+ \subseteq \mathcal{S}^+$, we shall derive a formula using only \mathcal{S} .

Finally, we get

$$\begin{aligned}
 & \prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}((n+n)!)-2E''_{q,t}(n!)} \\
 & \equiv_q \prod_{u \in [1, q-1]} \left(\prod_{t \in [1, 2u \pmod{q}] \cap \mathbb{Z}_q^*} t \right)^{\#(\mathcal{S}, \{u\})} \\
 & \quad \times \prod_{u \in [1, q-1]} \left(\prod_{t \in [u+1, q-1] \cap \mathbb{Z}_q^*} t^2 \right)^{\#(\mathcal{S}, \{u\})} \\
 & \quad \times \prod_{\substack{u \in [1, q-1] \\ 2u+1 \in \mathbb{Z}_q^*}} (2u+1 \pmod{q})^{\#(\bar{\mathcal{S}}, \{u\})},
 \end{aligned}$$

where $\bar{\mathcal{S}} = \{u = |\langle n_{k+i-1} \dots n_{i+1} n_i \rangle_p| : u \neq 0, u_0 \neq (p-1)/2 \text{ and } \kappa(n, n; i-1) = 1\}_{i \geq 0}$.

Note $\bar{\mathcal{S}} \subseteq \mathcal{S}$ and $\bar{\mathcal{S}}^+ = \{2u \pmod{q} : u \in \bar{\mathcal{S}}\}$.

- The formula $\prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}((n+n)!)-2E''_{q,t}(n!)}$ on the last page only depends on \mathcal{S} and $\bar{\mathcal{S}}$, and no more \mathcal{S}^+ and $\bar{\mathcal{S}}^+$.

- The formula $\prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}((n+n)!)-2E''_{q,t}(n!)}$ on the last page only depends on \mathcal{S} and $\bar{\mathcal{S}}$, and no more \mathcal{S}^+ and $\bar{\mathcal{S}}^+$.
- To evaluate $\prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}((n+n)!)-2E''_{q,t}(n!)}$ for a particular prime power q , we need to construct a table according to $u \in \mathbb{Z}_q^*$ for the following three values:

$$A = \prod_{t \in [1, 2u \pmod{q}] \cap \mathbb{Z}_q^*} t,$$

$$B = \left(\prod_{t \in [u+1, q-1] \cap \mathbb{Z}_q^*} t \right)^2 \quad \text{and}$$

$$C = 2u + 1 \pmod{q}.$$

Example: $c_{3212} \pmod{27}$

- Let $p = 3$, $k = 3$ and $n = 3212$. What is $c_{3212} \pmod{27}$?

Example: $c_{3212} \pmod{27}$

- Let $p = 3$, $k = 3$ and $n = 3212$. What is $c_{3212} \pmod{27}$?
- $[3212]_3 = \langle 1110\mathbf{1}222 \rangle_3$. So $\beta = 3$.

Example: $c_{3212} \pmod{27}$

- Let $p = 3$, $k = 3$ and $n = 3212$. What is $c_{3212} \pmod{27}$?
- $[3212]_3 = \langle 1110\mathbf{1}222 \rangle_3$. So $\beta = 3$.
- Then $\omega_p(c_{3212}) = C_p(n, n; \beta) = 1$.

Example: $c_{3212} \pmod{27}$

- Let $p = 3$, $k = 3$ and $n = 3212$. What is $c_{3212} \pmod{27}$?
- $[3212]_3 = \langle 1110\mathbf{1}222 \rangle_3$. So $\beta = 3$.
- Then $\omega_p(c_{3212}) = C_p(n, n; \beta) = 1$.
- $CF_q(c_n) \equiv_q \frac{1}{CF_q(n+1)} (-1)^{E'_q((n+n)!)} \times \prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}((n+n)!)-2E''_{q,t}(n!)}.$

Example: $c_{3212} \pmod{27}$

- Let $p = 3$, $k = 3$ and $n = 3212$. What is $c_{3212} \pmod{27}$?
- $[3212]_3 = \langle 1110\textcolor{red}{1}222 \rangle_3$. So $\beta = 3$.
- Then $\omega_p(c_{3212}) = C_p(n, n; \beta) = 1$.
- $CF_q(c_n) \equiv_q \frac{1}{CF_q(n+1)} (-1)^{E'_q((n+n)!)} \times \prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}((n+n)! - 2E''_{q,t}(n!))}.$
- In general, $CF_q(n+1) \equiv_q |\langle n_{\beta+k-1} \dots n_{\beta+1} (n_{\beta} + 1) \rangle_p|$.
In this case, $CF_q(3213) \equiv_{27} |\langle 10\textcolor{red}{2} \rangle_p| = 11$.

Example: $c_{3212} \pmod{27}$

- Let $p = 3$, $k = 3$ and $n = 3212$. What is $c_{3212} \pmod{27}$?
- $[3212]_3 = \langle 1110\textcolor{red}{1}222 \rangle_3$. So $\beta = 3$.
- Then $\omega_p(c_{3212}) = C_p(n, n; \beta) = 1$.
- $CF_q(c_n) \equiv_q \frac{1}{CF_q(n+1)} (-1)^{E'_q((n+n)!)} \times \prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}((n+n)! - 2E''_{q,t}(n!))}.$
- In general, $CF_q(n+1) \equiv_q |\langle n_{\beta+k-1} \dots n_{\beta+1} (n_{\beta} + 1) \rangle_p|$.
In this case, $CF_q(3213) \equiv_{27} |\langle 10\textcolor{red}{2} \rangle_p| = 11$.
- $E'_q((n+n)!) \equiv_2 C_p(n, n; k-1) = 2 \equiv_2 0$.

Here is the table for evaluating $\prod_{t \in \mathbb{Z}_{27}^*} t^{E''_{27,t}((2n)!) - 2E''_{27,t}(n!)}$.

u	1	2	3	4	5	6	7	8	9	10	11	12	13	...
A	2	8	13	26	17	25	14	8	1	2	17	13	26	...
B	1	7	7	19	4	4	10	1	1	10	7	7	1	...
C		5	7		11	13		17	19		23	25		...

$$A = \prod_{t \in [1, 2u \pmod{q}] \cap \mathbb{Z}_q^*} t,$$

$$B = \left(\prod_{t \in [u+1, q-1] \cap \mathbb{Z}_q^*} t \right)^2 \quad \text{and}$$

$$C = 2u + 1 \pmod{q}.$$

Here is the table for evaluating $\prod_{t \in \mathbb{Z}_{27}^*} t^{E''_{27,t}((2n)!) - 2E''_{27,t}(n!)}$.

u	\cdots	14	15	16	17	18	19	20	21	22	23	24	25	26
A	\cdots	2	8	13	26	17	25	14	8	1	2	17	13	26
B	\cdots	4	4	19	1	1	19	7	7	10	4	4	1	1
C	\cdots	2	4		8	10		14	16		20	22		26

$$A = \prod_{t \in [1, 2u \pmod{q}] \cap \mathbb{Z}_q^*} t,$$

$$B = \left(\prod_{t \in [u+1, q-1] \cap \mathbb{Z}_q^*} t \right)^2 \quad \text{and}$$

$$C = 2u + 1 \pmod{q}.$$

When $\kappa = 1$ and $u_0 \neq 1$, we shall use $A \cdot B \cdot C$; otherwise $A \cdot B$.

u	1	2	3	4	5	6	7	8	9	10	11	12	13
$A \cdot B$	2	2	10	8	14	19	5	8	1	20	11	10	26
$A \cdot B \cdot C$		10	16		19	4		1	19		10	7	
14	15	16	17	18	19	20	21	22	23	24	25	26	
8	5	4	26	17	16	17	2	10	8	14	13	26	
16	20		19	8		22	5		25	11		1	

When $\kappa = 1$ and $u_0 \neq 1$, we shall use $A \cdot B \cdot C$; otherwise $A \cdot B$.

u	1	2	3	4	5	6	7	8	9	10	11	12	13
$A \cdot B$	2	2	10	8	14	19	5	8	1	20	11	10	26
$A \cdot B \cdot C$		10	16		19	4		1	19		10	7	
	14	15	16	17	18	19	20	21	22	23	24	25	26
	8	5	4	26	17	16	17	2	10	8	14	13	26
	16	20		19	8		22	5		25	11		1

For our case, $[3212]_3 = \langle 11101222 \rangle_3$ and
 $\mathcal{S} = \{001, 011, 111, 110, 101, 012, 122, 222\}$.

When $\kappa = 1$ and $u_0 \neq 1$, we shall use $A \cdot B \cdot C$; otherwise $A \cdot B$.

u	1	2	3	4	5	6	7	8	9	10	11	12	13
$A \cdot B$	2	2	10	8	14	19	5	8	1	20	11	10	26
$A \cdot B \cdot C$		10	16		19	4		1	19		10	7	
	14	15	16	17	18	19	20	21	22	23	24	25	26
	8	5	4	26	17	16	17	2	10	8	14	13	26
	16	20		19	8		22	5		25	11		1

For our case, $[3212]_3 = \langle 11101222 \rangle_3$ and
 $\mathcal{S} = \{001, 011, 111, 110, 101, 012, 122, 222\}$.

We have $CF_{27}(c_{3212}) \equiv_{27} \frac{1}{11}(-1)^0 \times \prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}((n+n)!)-2E''_{q,t}(n!)}$.

When $\kappa = 1$ and $u_0 \neq 1$, we shall use $A \cdot B \cdot C$; otherwise $A \cdot B$.

u	1	2	3	4	5	6	7	8	9	10	11	12	13
$A \cdot B$	2	2	10	8	14	19	5	8	1	20	11	10	26
$A \cdot B \cdot C$		10	16		19	4		1	19		10	7	
	14	15	16	17	18	19	20	21	22	23	24	25	26
	8	5	4	26	17	16	17	2	10	8	14	13	26
	16	20		19	8		22	5		25	11		1

For our case, $[3212]_3 = \langle 11101222 \rangle_3$ and
 $\mathcal{S} = \{001, 011, 111, 110, 101, 012, 122, 222\}$.

We have $CF_{27}(c_{3212}) \equiv_{27} 5 \times \prod_{t \in \mathbb{Z}_q^*} t^{E''_{q,t}((n+n)!)-2E''_{q,t}(n!)}$.

When $\kappa = 1$ and $u_0 \neq 1$, we shall use $A \cdot B \cdot C$; otherwise $A \cdot B$.

u	1	2	3	4	5	6	7	8	9	10	11	12	13
$A \cdot B$	2	2	10	8	14	19	5	8	1	20	11	10	26
$A \cdot B \cdot C$		10	16		19	4		1	19		10	7	

14	15	16	17	18	19	20	21	22	23	24	25	26
8	5	4	26	17	16	17	2	10	8	14	13	26
16	20		19	8		22	5		25	11		1

For our case, $[3212]_3 = \langle 11101222 \rangle_3$ and

$\mathcal{S} = \{001, 011, 111, 110, 101, 012, 122, 222\}$.

So $u = |\langle 001 \rangle_3| = 1$ corresponding to 2 in the table.

We have $CF_{27}(c_{3212}) \equiv_{27} 5 \times (2 \times \cdots)$.

When $\kappa = 1$ and $u_0 \neq 1$, we shall use $A \cdot B \cdot C$; otherwise $A \cdot B$.

u	1	2	3	4	5	6	7	8	9	10	11	12	13
$A \cdot B$	2	2	10	8	14	19	5	8	1	20	11	10	26
$A \cdot B \cdot C$		10	16		19	4		1	19		10	7	
	14	15	16	17	18	19	20	21	22	23	24	25	26
	8	5	4	26	17	16	17	2	10	8	14	13	26
	16	20		19	8		22	5		25	11		1

For our case, $[3212]_3 = \langle 11101222 \rangle_3$ and

$\mathcal{S} = \{001, 011, 111, 110, 101, 012, 122, 222\}$.

So $u = |\langle 011 \rangle_3| = 4$ corresponding to 8.

We have $CF_{27}(c_{3212}) \equiv_{27} 5 \times (2 \cdot 8 \times \cdots)$.

When $\kappa = 1$ and $u_0 \neq 1$, we shall use $A \cdot B \cdot C$; otherwise $A \cdot B$.

u	1	2	3	4	5	6	7	8	9	10	11	12	13
$A \cdot B$	2	2	10	8	14	19	5	8	1	20	11	10	26
$A \cdot B \cdot C$		10	16		19	4		1	19		10	7	
	14	15	16	17	18	19	20	21	22	23	24	25	26
	8	5	4	26	17	16	17	2	10	8	14	13	26
	16	20		19	8		22	5		25	11		1

For our case, $[3212]_3 = \langle 11101222 \rangle_3$ and

$\mathcal{S} = \{001, 011, \mathbf{111}, 110, 101, 012, 122, 222\}$.

So $u = |\langle \mathbf{111} \rangle_3| = \mathbf{13}$ corresponding to **26**.

We have $CF_{27}(c_{3212}) \equiv_{27} 5 \times (2 \cdot 8 \cdot \mathbf{26} \times \cdots)$.

When $\kappa = 1$ and $u_0 \neq 1$, we shall use $A \cdot B \cdot C$; otherwise $A \cdot B$.

u	1	2	3	4	5	6	7	8	9	10	11	12	13
$A \cdot B$	2	2	10	8	14	19	5	8	1	20	11	10	26
$A \cdot B \cdot C$		10	16		19	4		1	19		10	7	
	14	15	16	17	18	19	20	21	22	23	24	25	26
	8	5	4	26	17	16	17	2	10	8	14	13	26
	16	20		19	8		22	5		25	11		1

For our case, $[3212]_3 = \langle 11101222 \rangle_3$ and

$\mathcal{S} = \{001, 011, 111, \mathbf{110}, 101, 012, 122, 222\}$.

So $u = |\langle \mathbf{110} \rangle_3| = \mathbf{12}$ with $\kappa = 1$ corresponding to $\mathbf{7}$.

We have $CF_{27}(c_{3212}) \equiv_{27} 5 \times (2 \cdot 8 \cdot 26 \cdot \mathbf{7} \times \dots)$.

When $\kappa = 1$ and $u_0 \neq 1$, we shall use $A \cdot B \cdot C$; otherwise $A \cdot B$.

u	1	2	3	4	5	6	7	8	9	10	11	12	13
$A \cdot B$	2	2	10	8	14	19	5	8	1	20	11	10	26
$A \cdot B \cdot C$		10	16		19	4		1	19		10	7	

14	15	16	17	18	19	20	21	22	23	24	25	26
8	5	4	26	17	16	17	2	10	8	14	13	26
16	20		19	8		22	5		25	11		1

For our case, $[3212]_3 = \langle 11101222 \rangle_3$ and

$\mathcal{S} = \{001, 011, 111, 110, 101, 012, 122, 222\}$.

So $u = |\langle 101 \rangle_3| = 10$ corresponding to 20. ($\kappa = 1$ but $u_0 = 1$)

We have $CF_{27}(c_{3212}) \equiv_{27} 5 \times (2 \cdot 8 \cdot 26 \cdot 7 \cdot 20 \times \dots)$.

When $\kappa = 1$ and $u_0 \neq 1$, we shall use $A \cdot B \cdot C$; otherwise $A \cdot B$.

u	1	2	3	4	5	6	7	8	9	10	11	12	13
$A \cdot B$	2	2	10	8	14	19	5	8	1	20	11	10	26
$A \cdot B \cdot C$		10	16		19	4		1	19		10	7	
	14	15	16	17	18	19	20	21	22	23	24	25	26
	8	5	4	26	17	16	17	2	10	8	14	13	26
	16	20		19	8		22	5		25	11		1

For our case, $[3212]_3 = \langle 11101222 \rangle_3$ and

$\mathcal{S} = \{001, 011, 111, 110, 101, 012, 122, 222\}$.

So $u = |\langle 012 \rangle_3| = 5$ with $ka = 1$ corresponding to 19.

We have $CF_{27}(c_{3212}) \equiv_{27} 5 \times (2 \cdot 8 \cdot 26 \cdot 7 \cdot 20 \cdot 19 \times \dots)$.

When $\kappa = 1$ and $u_0 \neq 1$, we shall use $A \cdot B \cdot C$; otherwise $A \cdot B$.

u	1	2	3	4	5	6	7	8	9	10	11	12	13
$A \cdot B$	2	2	10	8	14	19	5	8	1	20	11	10	26
$A \cdot B \cdot C$		10	16		19	4		1	19		10	7	
	14	15	16	17	18	19	20	21	22	23	24	25	26
	8	5	4	26	17	16	17	2	10	8	14	13	26
	16	20		19	8		22	5		25	11		1

For our case, $[3212]_3 = \langle 11101222 \rangle_3$ and

$\mathcal{S} = \{001, 011, 111, 110, 101, 012, 122, 222\}$.

So $u = |\langle 122 \rangle_3| = 17$ with $ka = 1$ corresponding to 19.

We have $CF_{27}(c_{3212}) \equiv_{27} 5 \times (2 \cdot 8 \cdot 26 \cdot 7 \cdot 20 \cdot 19 \cdot 19 \times \dots)$.

When $\kappa = 1$ and $u_0 \neq 1$, we shall use $A \cdot B \cdot C$; otherwise $A \cdot B$.

u	1	2	3	4	5	6	7	8	9	10	11	12	13
$A \cdot B$	2	2	10	8	14	19	5	8	1	20	11	10	26
$A \cdot B \cdot C$		10	16		19	4		1	19		10	7	
	14	15	16	17	18	19	20	21	22	23	24	25	26
	8	5	4	26	17	16	17	2	10	8	14	13	26
	16	20		19	8		22	5		25	11		1

For our case, $[3212]_3 = \langle 11101222 \rangle_3$ and

$\mathcal{S} = \{001, 011, 111, 110, 101, 012, 122, \mathbf{222}\}$.

So $u = |\langle \mathbf{222} \rangle_3| = \mathbf{26}$ corresponding to $\mathbf{26}$.

We have $CF_{27}(c_{3212}) \equiv_{27} 5 \times (2 \cdot 8 \cdot 26 \cdot 7 \cdot 20 \cdot 19 \cdot 19 \cdot \mathbf{26})$.

When $\kappa = 1$ and $u_0 \neq 1$, we shall use $A \cdot B \cdot C$; otherwise $A \cdot B$.

u	1	2	3	4	5	6	7	8	9	10	11	12	13
$A \cdot B$	2	2	10	8	14	19	5	8	1	20	11	10	26
$A \cdot B \cdot C$		10	16		19	4		1	19		10	7	
	14	15	16	17	18	19	20	21	22	23	24	25	26
	8	5	4	26	17	16	17	2	10	8	14	13	26
	16	20		19	8		22	5		25	11		1

For our case, $[3212]_3 = \langle 11101222 \rangle_3$ and
 $\mathcal{S} = \{001, 011, 111, 110, 101, 012, 122, 222\}$.

We have $CF_{27}(c_{3212}) \equiv_{27} 4$.

When $\kappa = 1$ and $u_0 \neq 1$, we shall use $A \cdot B \cdot C$; otherwise $A \cdot B$.

u	1	2	3	4	5	6	7	8	9	10	11	12	13
$A \cdot B$	2	2	10	8	14	19	5	8	1	20	11	10	26
$A \cdot B \cdot C$		10	16		19	4		1	19		10	7	
	14	15	16	17	18	19	20	21	22	23	24	25	26
	8	5	4	26	17	16	17	2	10	8	14	13	26
	16	20		19	8		22	5		25	11		1

For our case, $[3212]_3 = \langle 11101222 \rangle_3$ and
 $\mathcal{S} = \{001, 011, 111, 110, 101, 012, 122, 222\}$.

We have $CF_{27}(c_{3212}) \equiv_{27} 4$. Then $c_{3212} \equiv_{27} 3^1 \times 4 = 12$.

Catalan Numbers Modulo a Prime Power

└ Catalan numbers modulus an odd prime power

└ Example: $c_{3212} \pmod{27}$

u	1	2	3	4	5	6	7	8	9	10	11	12	13
$A \cdot B$	2	2	10	8	14	19	5	8	1	20	11	10	26
$A \cdot B \cdot C$		10	16		19	4		1	19		10	7	■
14	15	16	17	18	19	20	21	22	23	24	25	26	
8	5	4	26	17	16	17	2	10	8	14	13	26	
16	20		19	8		22	5		25	11		1	

Lemma

$A \cdot B \equiv_q \pm 1$ and $A \cdot B \cdot C \equiv_q \pm 1$ for both $u = (q-1)/2$ and $u = q-1$.

Given $n \in \mathbb{N}$, let \bar{n} be the integer such that $[\bar{n}]_2$ is obtained by the following rules.

- If the rightmost 0 run and $p-1$ run of form the $[n]_2 = \langle \dots 0^{\beta'} (p-1)^{\beta} \rangle_p$ with $\beta, \beta' \geq k+1$, let us truncate their to length k , otherwise keep it the same.
- For any other run of 0 and $(p-1)/2$ of $[n]_2$ with length $\geq k+1$, truncate them to be length of the same parity as k or $k-1$.

Theorem

Let $n, k \in \mathbb{N}$ with $k \geq 3$. We have

$$c_n \equiv_{2^k} \begin{cases} c_{\bar{n}} & \text{for } d(\alpha) \leq k-1, \text{ and} \\ 0 & \text{for } d(\alpha) \geq k. \end{cases}$$

Example.

$$c_{\langle 3330006 \rangle}_7 \equiv_{49} 43,$$

$$c_{\langle 30006 \rangle}_7 \equiv_{49} 43,$$

$$c_{\langle 3006 \rangle}_7 \equiv_{49} 43,$$

$$c_{\langle 306 \rangle}_7 \equiv_{49} 15,$$

$$c_{\langle 3066 \rangle}_7 \equiv_{49} 1,$$

$$c_{\langle 30666 \rangle}_7 \equiv_{49} 1,$$

$$c_{\langle 33306 \rangle}_7 \equiv_{49} 15,$$

$$c_{\langle 3306 \rangle}_7 \equiv_{49} 34.$$

Example.

$$c_{\langle 3330006 \rangle_7} \equiv_{49} 43,$$

$$c_{\langle 30006 \rangle_7} \equiv_{49} 43,$$

$$c_{\langle 3006 \rangle_7} \equiv_{49} 43,$$

$$c_{\langle 306 \rangle_7} \equiv_{49} 15,$$

$$c_{\langle 3066 \rangle_7} \equiv_{49} 1,$$

$$c_{\langle 30666 \rangle_7} \equiv_{49} 1,$$

$$c_{\langle 33306 \rangle_7} \equiv_{49} 15,$$

$$c_{\langle 3306 \rangle_7} \equiv_{49} 34.$$

The End!