สมภาคของคุมเมอร์สำหรับจำนวนเชิงแบบฉบับ

นายสุปรีดี แดงสกุล

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์

คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2551

KUMMER'S CONGRUENCES FOR CLASSICAL NUMBERS

Mr. Supreedee Dangskul

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Mathematics

Department of Mathematics
Faculty of Science
Chulalongkorn University

Academic Year 2008

Thesis Title	KUMMER'S CONGRUENCES FOR CLASSICAL NUMBERS
By	Mr. Supreedee Dangskul
Field of Study	Mathematics
Thesis Principal Advisor	Tuangrat Chaichana, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

.... Dean of the Faculty of Science

(Professor Supot Hannongbua, Dr.rer.nat.)

THESIS COMMITTEE

.... Chairman

(Associate Professor Ajchara Harnchoowong, Ph.D.)

.... Thesis Principal Advisor

(Tuangrat Chaichana, Ph.D.)

.... Member

(Yotsanan Meemark, Ph.D.)

สุปรีดี แดงสกุล : สมภาคของคุมเมอร์สำหรับจำนวนเชิงแบบฉบับ (KUMMER'S CONGRUENCES FOR CLASSICAL NUMBERS) อ.ที่ปรึกษาวิทยานิพนธ์หลัก : ดร. ตวงรัตน์ ไชยชนะ, 42 หน้า.

ในวิทยานิพนธ์ฉบับนี้เราศึกษาสมภาคแบบพิเศษที่เรียกว่า สมภาคของคุมเมอร์ ซึ่งในที่นี้เราได้จำแนกออกเป็นสามแบบ ได้แก่ สมภาคของคุมเมอร์แบบที่ศูนย์ สมภาคของคุมเมอร์แบบที่หนึ่ง และสมภาคของคุมเมอร์แบบที่สอง โดยแสดงบางแง่มุมที่น่าสนใจ ความซับซ้อน รวมถึงความสัมพันธ์ที่เกี่ยวข้องกับสมภาคของคุมเมอร์ทั้งสามแบบข้างต้น นอกจากนี้เราได้ขยายเอกลักษณ์ที่สำคัญที่ใช้ในการพิสูจน์สมบัติเชิงสมภาคของคุมเมอร์สำหรับจำนวนแบร์นูลลี

ภาควิชา : ...**คณิตศาสตร์**... ลายมือชื่อนิสิต ......สุปรีดี แดงสกุล......
สาขาวิชา : ...**คณิตศาสตร์**... ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก ......ตวงรัตน์ ไชยชนะ......
ปีการศึกษา : ...2551...

4872521323 : MAJOR MATHEMATICS
KEYWORDS : KUMMER'S CONGRUENCE

SUPREEDEE DANGSKUL : KUMMER'S CONGRUENCES FOR CLASSICAL NUMBERS. THESIS PRINCIPAL ADVISOR : TUANGRAT CHAICHANA, Ph.D. 42 pp.

In this thesis, we study a special kind of congruences, called Kummer's congruences, which is here classified into three types, namely, Kummer's congruences of a zeroth kind, Kummer's congruences of a first kind and Kummer's congruences of a second kind. Some interesting aspects concerning congruences of each type and their complexity including some relationships among those three types are studied. A crucial identity for Bernoulli numbers employed to prove their Kummer's congruential properties is generalized.

Department : ...Mathematics... Student's Signature : Supreedee Dangskul
Field of Study : ...Mathematics... Principal Advisor's Signature : T. Chaichana
Academic Year : ....2008..........

ACKNOWLEDGEMENTS

I feel sincerely grateful to Dr. Tuangrat Chaichana, my thesis advisor, and, unforgettably, Professor Dr. Vichian Laohakosol for their great suggestions to my thesis as well as encouraging me to struggle troubles and difficulties throughout my graduate study. I also would like to thank Associate Professor Dr. Ajchara Harnchoowong and Dr. Yotsanan Meemark, my thesis committee, for giving me their time to read and check my thesis.

Finally, I would like to express all of my extremely deeply true indebtedness to my beloved warm family for the financial support.

CONTENTS

CHAPTER I

Introduction

In 1851, Kummer proved, see [7], a well-known congruence for Bernoulli numbers, B_n, of the the form

$$\frac{B_{n+p-1}}{n+p-1} \equiv \frac{B_n}{n}\ (mod\ p)$$

for all $n > 1$, where p is a prime and $p-1 \nmid n$. This originates the term Kummer's congruence which, so far, has been used in various meanings. There have been a number of papers using the term Kummer's congruence without a rigorous definition, for instance, the congruences for Euler numbers in the even-suffix notation, E_n, of the following forms

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}E_{n+s(p-1)} \equiv 0\ (mod\ p^r),$$

see [4], and

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}E_p^{r-s}E_{n+s(p-1)} \equiv 0\ (mod\ p^r),$$

see [3], where $n \geq r$ and p is an odd prime, are both referred to as Kummer's congruences. However, a classification has appeared in Stevens'work, see e.g. Stevens [9], but, unfortunately, it is not commonly used.

In this thesis, we first make precise the definition of Kummer's congruence by categorizing it into three types, referred to as Kummer's congruences of a zeroth kind, Kummer's congruences of a first kind and Kummer's congruences of a second kind and then study each type as well as relationships among them.

Our setting here consists of an integral domain R that contains the ring of all integers $\mathbb{Z}$. Congruences are here considered ideal theoretically.

Definition 1.1. *Let p be a fixed prime, $r \in \mathbb{N}$ and (a_n) a sequence in R. A Kummer's congruence of a zeroth kind is a congruence of the form*

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}a_{n+s(p-1)} \equiv 0 \ (mod\ p^r),$$

a Kummer's congruence of a first kind is a congruence of the form

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}a_p^{r-s}a_{n+s(p-1)} \equiv 0 \ (mod\ p^r)$$

and a Kummer's congruence of a second kind is a congruence of the form

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}a_p^{r-s}a_{n+sp} \equiv 0 \ (mod\ p^r)$$

where the free parameters n, r of each type may be subject to its additional requirements. Sometimes, the last type of Kummer's congruences (of a second kind) is referred to the form

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}a_p^{r-s}a_{n+sp} \equiv 0 \ (mod\ p^{r_1}),$$

where $r_1 = [\frac{r+1}{2}]$, and hereby called a weak Kummer's congruence of a second kind.

The following are examples of three types of Kummer's congruences with different conditions on the free parameters n and r.

Example 1.2. *Here, let $R = \mathbb{Z}$, $a_n = n$, $b_n = 1$ and $c_n = 2^n$. Then we have*

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}a_{n+s(p-1)} \equiv 0 \ (mod\ p^r)$$

where $n \geq 0$ and $r \geq 2$,

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}b_p^{r-s}b_{n+s(p-1)} \equiv 0 \ (mod\ p^r)$$

where $n, r \geq 0$ and

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}c_p^{r-s}c_{n+sp} \equiv 0 \ (mod\ p^r)$$

where $n, r \geq 0$.

In Chapter II, we introduce the usual differrence operator and prove their basic properties. Then we generalize the main identity employed to prove a Kummer's congruence of a zeroth kind for Bernoulli numbers.

In Chapter III, we consider Hurwitz series equipped with an operator Ω_p, study Snyder's method and then derive a criterion for a sequence to satisfy a Kummer's congruence of a first kind. Snyder's elegant technique is elaborately given in detail.

In Chapter IV, we deal with weak Kummer's congruences of a second kind. The proof is based on difference equations and a number of identities. An example of weak Kummer's congruences of a second kind is also given.

In the final chapter, Chapter V, we reveal some relationships among those three types of Kummer's congruences which can be viewed as common examples.

CHAPTER II

Kummer's congruences of a zeroth kind

In [6], Johnson used the $(p-1)$st roots of unity in $\mathbb{Z}_p$, the ring of p-adic integers, to prove congruences for Bernoulli numbers B_n. One such congruence is

$$\sum_{t=0}^{n}(-1)^{n-t}\binom{n}{t}\beta_{2k+(i+t)(p-1)} \equiv \ 0(mod\ p^n) \tag{2.1}$$

where $p \geq n+3$, $2k > n \geq 1$ and β_r are defined by

$$\beta_r = \begin{cases} B_r/r, & p-1 \nmid r \\ (B_r + p^{-1} - 1)/r, & p-1 | r. \end{cases} \tag{2.2}$$

The above congruence is deduced directly by the recursion

$$\beta_r + \sum_{a=1}^{p-1} a^{r-1}t(a) + \sum_{j=2}^{r}\frac{1}{r}\binom{r}{j}p^{j-1}\left(\frac{B_{r+1-j}}{r+1-j} + \sum_{a=1}^{p-1}a^{r-j}t(a)^j\right) + \frac{p^r}{(r+1)r} = 0,$$

where $r \geq 1$, using properties of the usual differrence operator, introduced soon in the first section.

Our goal of this chapter is to prove analogous results for sequences satisfying generalized recursion of the form

$$\beta_r + \sum_{j=2}^{r} f_{j-1}(r)\frac{p^{j-1}}{j!}\beta_{r+1-j} + \sum_{j=1}^{r} g_{j-1}(r)\frac{p^{j-1}}{j!}\sum_{s=1}^{S}c_{s,j}a_s^{r-j} + \sum_{j=2}^{r}h_{j-2}(r)\frac{p^{j-2}}{j!} + d\frac{p^r}{(r+1)r} = 0.$$

2.1 Difference operator

Let $x_1, x_2, \ldots$ be a sequence in any ring. Define the operator Δ_i by

$$\Delta_i^0 x_i = x_i\ ,\ \Delta_i^1 x_i = \Delta_i x_i = x_{i+1} - x_i$$

and

$$\Delta_i^n x_i = \Delta_i^1 \left(\Delta_i^{n-1} x_i\right) \quad (n \geq 2).$$

To avoid ambiguity, we use the subscript i in the operator to remind that the operator effects only to the terms having index i in the sequence.

It is easily checked that the operator Δ_i satisfies a linear property and the associative law, i.e., $\Delta_i^m \Delta_i^n = \Delta_i^{m+n}$. The following proposition summarizes some well-known properties of Δ_i.

Proposition 2.1. *For any integer $n \geq 0$, we have*

(i) $\Delta_i^n x_i = \displaystyle\sum_{t=0}^{n} (-1)^{n-t} \binom{n}{t} x_{i+t}$;

(ii) $\Delta_i^n (x_i y_i) = \displaystyle\sum_{t=0}^{n} \binom{n}{t} \left(\Delta_i^t x_i\right) \left(\Delta_i^{n-t} y_{i+t}\right)$ *(Leibniz's rule);*

(iii) if x_i is a polynomial in i of degree $< n$, then $\Delta_i^n x_i = 0$.

Proof. We use induction on n to show (i). This is easy for $n = 0$. Suppose that (i) is true for n. Then

$$\begin{aligned}
\Delta_i^{n+1} x_i &= \Delta_i \left(\Delta_i^n x_i\right) \\
&= \Delta_i \left(\sum_{t=0}^{n} (-1)^{n-t} \binom{n}{t} x_{i+t}\right) \\
&= \sum_{t=0}^{n} (-1)^{n-t} \binom{n}{t} x_{i+t+1} - \sum_{t=0}^{n} (-1)^{n-t} \binom{n}{t} x_{i+t} \\
&= x_{i+n+1} + (-1)^{n+1} x_i + \sum_{t=1}^{n} (-1)^{n+1-t} \left(\binom{n}{t} + \binom{n}{t-1}\right) x_{i+t} \\
&= \sum_{t=0}^{n+1} (-1)^{n+1-t} \binom{n+1}{t} x_{i+t}.
\end{aligned}$$

To prove (ii), we also use induction on n. For $n = 0$, this follows from the definition of the difference operator. Suppose that (ii) holds for n. To show (ii) for $n+1$, we easily have, by the induction hypothesis, that

$$\begin{aligned}
\Delta_i^{n+1}(x_i y_i) &= \Delta_i\left(\sum_{t=0}^{n}\binom{n}{t}\left(\Delta_i^t x_i\right)\left(\Delta_i^{n-t} y_{i+t}\right)\right)\\
&= \sum_{t=0}^{n}\binom{n}{t}\left(\Delta_i^t x_{i+1}\right)\left(\Delta_i^{n-t} y_{i+1+t}\right) - \sum_{t=0}^{n}\binom{n}{t}\left(\Delta_i^t x_i\right)\left(\Delta_i^{n-t} y_{i+t}\right)\\
&= \sum_{t=0}^{n}\binom{n}{t}\{\left(\Delta_i^t x_{i+1}\right)\left(\Delta_i^{n-t} y_{i+1+t}\right) - \left(\Delta_i^t x_i\right)\left(\Delta_i^{n-t} y_{i+1+t}\right)\\
&\qquad\qquad + \left(\Delta_i^t x_i\right)\left(\Delta_i^{n-t} y_{i+1+t}\right) - \left(\Delta_i^t x_i\right)\left(\Delta_i^{n-t} y_{i+t}\right)\}\\
&= \sum_{t=0}^{n}\binom{n}{t}\left(\Delta_i^{t+1} x_i\right)\left(\Delta_i^{n-t} y_{i+1+t}\right) + \sum_{t=0}^{n}\binom{n}{t}\left(\Delta_i^t x_i\right)\left(\Delta_i^{n+1-t} y_{i+t}\right)\\
&= \left(\Delta_i^{n+1} x_i\right) y_{i+1+n} + x_i\left(\Delta_i^{n+1} y_i\right)\\
&\qquad\qquad + \sum_{t=1}^{n}\left(\Delta_i^t x_i\right)\left(\Delta_i^{n+1-t} y_{i+t}\right)\left(\binom{n}{t} + \binom{n}{t-1}\right)\\
&= \sum_{t=0}^{n+1}\binom{n+1}{t}\left(\Delta_i^t x_i\right)\left(\Delta_i^{n+1-t} y_{i+t}\right).
\end{aligned}$$

To show (iii), it suffices to check that $\Delta_i^n\left(i^m\right) = 0$, for each integer m with $0 \le m < n$. It is obvious for $n = 0$. Suppose that (iii) is true for n. Now let $0 \le m < n+1$. Then, by the induction hypothesis, $\Delta_i^{n+1}\left(i^m\right) = \Delta_i\left(\Delta_i^n\left(i^m\right)\right) = 0$ for $0 \le m < n$. If $m = n$, we have

$$\Delta_i^{n+1}\left(i^n\right) = \Delta_i^n\left((i+1)^n - i^n\right) = \sum_{j=0}^{n-1}\binom{n}{j}\Delta_i^n\left(i^j\right) = 0.$$

□

2.2 Main theorems

Let p be a prime ≥ 5, $r \in \mathbb{N}$ and $\beta_1, \beta_2, \ldots,$ a sequence satisfying

$$\beta_r + \sum_{j=2}^{r} f_{j-1}(r)\frac{p^{j-1}}{j!}\beta_{r+1-j}$$

$$+ \sum_{j=1}^{r} g_{j-1}(r)\frac{p^{j-1}}{j!}\sum_{s=1}^{S} c_{s,j} a_s^{r-j} + \sum_{j=2}^{r} h_{j-2}(r)\frac{p^{j-2}}{j!} + d\frac{p^r}{(r+1)r} = 0 \tag{2.3}$$

where $f_{j-1}(r)$ and $g_{j-1}(r)$ are polynomials in r of degree $\leq j-1$ having coefficients in $\mathbb{Z}_p$ whereas $h_{j-2}(r)$ have degree $\leq j-2$, $a_s \in \mathbb{Z}$ with $\gcd(a_s, p) = 1$, $S \in \mathbb{N}$ and $c_{s,j}, d \in \mathbb{Z}_p$.

For $x \in \mathbb{Z}_p$, we let $e_p(x)$ be the largest exponent of prime p that divides x. The valuation e_p is regularly used for the rest of this chapter.

Lemma 2.2. *For $j \geq 1$, we have*

$$e_p\left(\frac{p^j}{j!}\right) > \left(\frac{p-2}{p-1}\right) j.$$

Proof. Clearly, $e_p\left(\frac{p^j}{j!}\right) = j - e_p(j!)$. The lemma follows from a well-known result that

$$e_p(j!) = \frac{j - \sum}{p-1}$$

where $\sum$ is the sum of all digits of j represented in base p. Since $\sum \geq 1$, we obtain

$$e_p\left(\frac{p^j}{j!}\right) = j - e_p(j!) = j - \frac{j-\sum}{p-1} \geq j - \frac{j-1}{p-1} > \left(\frac{p-2}{p-1}\right) j.$$

$\square$

Lemma 2.3. *For $r \geq 1$, we have $\beta_r \in \mathbb{Z}_p$.*

Proof. It is obvious, from the equation (2.3), that

$$\beta_1 = -g_0(r) \sum_{s=1}^{S} c_{s,1} - d\left(\frac{p}{2}\right) \in \mathbb{Z}_p.$$

Suppose that $\beta_i \in \mathbb{Z}_p$ for all $1 \leq i \leq r-1$. Lemma 2.2 gives us $e_p(\frac{p^{j-1}}{j!}) \geq 1$ for $j \geq 2$ and $e_p(\frac{p^{j-2}}{j!}) \geq 0$ for $j \geq 2$ which imply that the three middle summations of (2.3) belong to $\mathbb{Z}_p$. Now, it remains to check that $d\frac{p^r}{(r+1)r} \in \mathbb{Z}_p$. Since

$$\begin{aligned} e_p\left(\frac{p^r}{(r+1)r}\right) &\geq e_p\left(\frac{p^r}{(r+1)!}\right) \\ &> \left(\frac{p-2}{p-1}\right)(r+1) - 1 \\ &\geq \left(\frac{3}{4}\right)(2) - 1 = \frac{1}{2}, \end{aligned}$$

this establishes the lemma. $\square$

Theorem 2.4. *For $r \geq 2$, we have $\beta_r \equiv \beta_{r+p-1}$ (mod p).*

Proof. We easily obtain, from Lemma 2.2, that $e_p(\frac{p^{j-1}}{j!}) \geq 1$ for $j \geq 2$ and $e_p(\frac{p^{j-2}}{j!}) \geq 1$ for $j \geq 3$. Then the equation (2.1) becomes

$$\beta_r + g_0(r)\sum_{s=1}^{S} c_{s,1}a_s^{r-1} + \frac{h_0(r)}{2} \equiv 0 \ (mod\ p).$$

By the Fermat's little theorem, it follows from $\gcd(a_s, p) = 1$ that

$$\beta_r \equiv -g_0(r)\sum_{s=1}^{S} c_{s,1}a_s^{r-1+p-1} - \frac{h_0(r)}{2} \equiv \beta_{r+p-1} \ (mod\ p).$$

□

Theorem 2.5. *Let $n \leq p-3$. For $k > n \geq 1$, $\Delta_i^n \beta_{k+i(p-1)} \equiv 0$ (mod p^n).*

Proof. We show the theorem by induction on n. For $n = 1$, it follows by Theorem 2.4 that, for each $k > 1$.

$$\Delta_i \beta_{k+i(p-1)} = \beta_{k+i(p-1)} - \beta_{k+(i+1)(p-1)} \equiv 0 \ (mod\ p).$$

Suppose that the theorem holds up to the value $n-1$, i.e., for each $1 \leq m \leq n-1$, if $k' > m \geq 1$, then

$$\Delta_i^m \beta_{k'+i(p-1)} \equiv 0 \ (mod\ p^m)$$

for all $i \geq 1$. To show the induction step, we let $k > n \geq 1$ and use the equation (2.3) with $r = k + i(p-1)$. Now, we aim to show that all summations and single terms but the first in the equation (2.3) are congruent to 0 modulo p^n after taking Δ_i^n.

To deal with the second summation

$$\sum_{j=2}^{r} f_{j-1}(r)\frac{p^{j-1}}{j!}\beta_{r+1-j}$$

in the equation (2.3), we separate it into 2 cases. If $n+1 \leq j \leq r$, then

$$e_p\left(\frac{p^{j-1}}{j!}\right) > \left(\frac{p-2}{p-1}\right)j - 1 \geq \left(\frac{n+1}{n+2}\right)(n+1) - 1$$
$$= \frac{n^2+n-1}{n+2} = n - \frac{n+1}{n+2}$$

and hence

$$e_p\left(\frac{p^{j-1}}{j!}\right) \geq n.$$

Now let $2 \leq j \leq n$. Since $j \leq n < p$, we have $p \nmid j!$, that is, $e_p\left(\frac{p^{j-1}}{j!}\right) = j-1$. Observe that, for each $2 \leq j \leq n$,

$$\begin{aligned}
\Delta_i^n f_{j-1}(r)\beta_{r+1-j} &= \sum_{t=0}^{n} \binom{n}{t} \Delta_i^t f_{j-1}(r) \Delta_i^{n-t} \beta_{k+(i+t)(p-1)+1-j} \\
&= \sum_{t=0}^{j-1} \binom{n}{t} \Delta_i^t f_{j-1}(r) \Delta_i^{n-t} \beta_{k+(i+t)(p-1)+1-j}.
\end{aligned}$$

We are reduced to show only

$$\Delta_i^{n-t} \beta_{k+(i+t)(p-1)+1-j} \equiv 0 \ (mod \ p^{n-j+1}).$$

where $0 \leq t \leq j-1$. The case of $t = 0$ is considered separately. Since

$$k+1-j > n-j+1,$$

the induction hypothesis implies that

$$\Delta_i^{n-j+1} \beta_{k+i(p-1)+1-j} \equiv 0 \ (mod \ p^{n-j+1})$$

and thus

$$\Delta_i^n \beta_{k+i(p-1)+1-j} = \Delta_i^{j-1} \left(\Delta_i^{n-j+1} \beta_{k+i(p-1)+1-j}\right) \equiv 0 \ (mod \ p^{n-j+1}).$$

As in the previous case, if $1 \leq t \leq j-1$, then

$$\Delta_i^{n-t} \beta_{k+(i+t)(p-1)+1-j} \equiv 0 \ (mod \ p^{n-t})$$

because $k + t(p-1) + 1 - j > n - t$.

We now come to the next summation. As above, we do not repeat for the case of $n+1 \leq j \leq r$. Since $e_p\left(\frac{p^{j-1}}{j!}\right) \geq j-1$ for all $2 \leq j \leq n$, it suffices to show that

$$\Delta_i^n \left(g_{j-1}(r) a_s^{k+i(p-1)-j}\right) \equiv 0 \ (mod \ p^{n-j+1}).$$

But

$$\Delta_i^n \left(g_{j-1}(r)a_s^{i(p-1)}\right) = \sum_{t=0}^{n} \binom{n}{t} \left(\Delta_i^t g_{j-1}(r)\right) \left(\Delta_i^{n-t} a_s^{(i+t)(p-1)}\right)$$

$$= \sum_{t=0}^{j-1} \binom{n}{t} \left(\Delta_i^t g_{j-1}(r)\right) \left(\Delta_i^{n-t} a_s^{(i+t)(p-1)}\right)$$

and

$$\Delta_i^{n-t} \left(a_s^{i(p-1)}\right) = \sum_{l=0}^{n-t} (-1)^{n-t-l} \binom{n-t}{l} a_s^{(i+l)(p-1)}$$

$$= a_s^{i(p-1)} \left(a_s^{p-1} - 1\right)^{n-t} \equiv 0 \ (mod\ p^{n-t}).$$

For $j = 1$, we only consider $g_0(r) \sum_{s=1}^{S} c_{s,1} a_s^{r-1}$. Notice that

$$\Delta_i^n (g_0(r)a_s^{i(p-1)}) = g_0(r)\Delta_i^n a_s^{i(p-1)}$$

$$\equiv 0 \ (mod\ p^n).$$

Then

$$\Delta_i^n \left(\sum_{j=1}^{r} g_{j-1}(r) \frac{p^{j-1}}{j!} \sum_{s=1}^{S} c_{s,j} a_s^{r-j} \right) \equiv 0 \ (mod\ p^n).$$

Now consider the forth summation in the equation (2.3)

$$\sum_{j=2}^{r} h_{j-2}(r) \frac{p^{j-2}}{j!}.$$

Clearly, if $2 \leq j \leq n+1$, then

$$\Delta_i^n \left(h_{j-2}(r)\right) = 0$$

and thus

$$\Delta_i^n \left(\sum_{j=2}^{r} h_{j-2}(r) \frac{p^{j-2}}{j!} \right) = \frac{p^{j-2}}{j!} \sum_{j=2}^{r} \Delta_i^n \left(h_{j-2}(r)\right) = 0,$$

by Proposition 2.1 (iii). If $n+2 \leq j \leq r$, then it follows from

$$e_p \left(\frac{p^{j-2}}{j!} \right) > \left(\frac{p-2}{p-1} \right) j - 2$$

$$\geq \left(\frac{n+1}{n+2} \right) (n+2) - 2 = n - 1.$$

that

$$\frac{p^{j-2}}{j!} \equiv 0 \ (mod \ p^n).$$

Finally, for the last term, since

$$\begin{aligned} e_p\left(\frac{p^r}{(r+1)r}\right) &\geq e_p\left(\frac{p^r}{(r+1)!}\right) > \left(\frac{p-2}{p-1}\right)(r+1)-1 \\ &\geq \left(\frac{n+1}{n+2}\right)(k+i(p-1)+1)-1 > \left(\frac{n+1}{n+2}\right)(n+2)-1, \end{aligned}$$

we have

$$e_p\left(\frac{p^r}{(r+1)r}\right) \geq n,$$

i.e.,

$$d\frac{p^r}{(r+1)r} \equiv 0 \ (mod \ p^n).$$

□

We remark that the lemmas and theorems, stated in this section, still hold if $\beta_1 \in \mathbb{Z}_p$ (other than β_1 from substituting $r = 1$ in (2.3)) and the equation (2.3) is true for all $r \geq 2$. Their proofs are the same as above and so are omitted here.

An application concerning Bernoulli numbers will be given in the following section.

2.3 Bernoulli numbers and the $(p-1)$st roots of unity

Definition 2.6. *The Bernoulli numbers $B_0, B_1, B_2, \ldots$ are defined by $B_0 = 1$ and the recursion*

$$1 + \sum_{j=1}^{r} \binom{r+1}{j} B_{r+1-j} = 0. \tag{2.4}$$

A fact about the Euler-Maclaurin summation formula is established now.

Proposition 2.7. *The Euler-Maclaurin summation formula*

$$(r+1)\sum_{a=1}^{n-1} a^r = \sum_{j=1}^{r} \binom{r+1}{j} B_{r+1-j} n^j + n^{r+1}, \tag{2.5}$$

for $n, r \geq 1$, is equivalent to (2.4).

Proof. Setting $n = 1$ shows that (2.5) implies (2.4). Assume (2.4) which is also the basis step for showing (2.5) by induction on n. Now suppose that (2.5) holds for a value n. Then

$$\begin{aligned}
&\sum_{j=1}^{r}\binom{r+1}{j}B_{r+1-j}(n+1)^{j}+(n+1)^{r+1}\\
&\quad=\sum_{j=1}^{r}\binom{r+1}{j}B_{r+1-j}\sum_{s=0}^{j}\binom{j}{s}n^{s}+\sum_{t=0}^{r+1}\binom{r+1}{t}n^{t}\\
&\quad=(r+1)\sum_{a=1}^{n-1}a^{r}+\sum_{j=1}^{r}\binom{r+1}{j}B_{r+1-j}\sum_{s=0}^{j-1}\binom{j}{s}n^{s}+\sum_{t=0}^{r}\binom{r+1}{t}n^{t}\\
&\quad=(r+1)\sum_{a=1}^{n-1}a^{r}+\sum_{s=0}^{r-1}\binom{r+1}{s}n^{s}\sum_{j=s+1}^{r}\binom{r+1-s}{j-s}B_{r+1-j}+\sum_{t=0}^{r}\binom{r+1}{t}n^{t}\\
&\quad=(r+1)\sum_{a=1}^{n-1}a^{r}+\sum_{s=0}^{r-1}\binom{r+1}{s}n^{s}\sum_{j=1}^{r-s}\binom{r+1-s}{j}B_{r+1-s-j}+\sum_{t=0}^{r}\binom{r+1}{t}n^{t}\\
&\quad=(r+1)\sum_{a=1}^{n-1}a^{r}-\sum_{s=0}^{r-1}\binom{r+1}{s}n^{s}+\sum_{t=0}^{r}\binom{r+1}{t}n^{t}\\
&\quad=(r+1)\sum_{a=1}^{n}a^{r}.
\end{aligned}$$

This proves the assertion for $n + 1$ and therefore the proposition. □

Let U denote the group of all units in the ring $\mathbb{Z}_p$. We know, from [1], that the set V consisting of all $(p-1)$st roots of unity in $\mathbb{Z}_p$ forms a cyclic mutiplicative subgroup of U of order $p-1$. Also, for $r \geq 1$, we have

$$\sum_{v\in V} v^{r} = \begin{cases} 0, & p-1 \nmid r \\ p-1, & p-1 | r. \end{cases} \tag{2.6}$$

Any $x \in \mathbb{Z}_p$ has the p-adic representation

$$x = \sum_{n=0}^{\infty} x_n p^n,$$

where the x_n are integers satisfying $0 \leq x_n < p$ for all $n \geq 0$. Whenever $x \in \mathbb{Z}_p$, we let x_n denote the coefficient of p^n in the p-adic representation of x.

For any rational integer a, $1 \leq a \leq p-1$, let $v(a)$ be the unique element of V with $v(a) \equiv a$ $(mod\ p)$. In particular, $v(a)_0 = a$.

Now, we write the p-adic expansion for $v = v(a)$ in V as follows:

$$v = v(a) = a + t(a)p \tag{2.7}$$

where $t(a) = \displaystyle\sum_{n=1}^{\infty} v(a)_n p^{n-1}$. Expanding the rth power of (2.7) and using the equation (2.5) with $n = p$, we obtain, for $r \geq 1$,

$$\sum_{v \in V} v^r = \sum_{j=1}^{r} \binom{r}{j} p^j \left(\frac{B_{r+1-j}}{r+1-j} + \sum_{a=1}^{p-1} a^{r-j} t(a)^j \right) + \frac{p^r}{r+1}. \tag{2.8}$$

Together with equation (2.6), we get

$$\beta_r + \sum_{a=1}^{p-1} a^{r-1} t(a) + \sum_{j=2}^{r} \frac{1}{r} \binom{r}{j} p^{j-1} \left(\frac{B_{r+1-j}}{r+1-j} + \sum_{a=1}^{p-1} a^{r-j} t(a)^j \right) + \frac{p^r}{(r+1)r} = 0, \tag{2.9}$$

where $r \geq 1$, and β_r is given by

$$\beta_r = \begin{cases} B_r/r, & p-1 \nmid r \\ (B_r + p^{-1} - 1)/r, & p-1 | r. \end{cases}$$

Theorem 2.8. *The sequence β_r defined as* (2.9) *satisfies the equation* (2.3)*. In particular, the lemmas and theorems in the previous section are valid.*

Proof. Putting $f_{j-1}(r) = (r-1)\cdots(r-j+1) = g_{j-1}(r)$ for $2 \leq j \leq r$, $g_0(r) = 1$,

$$h_{j-2} = \begin{cases} (p-1)(r-1)\cdots(r-j+2), & p-1 | r+1-j \\ 0 & p-1 \nmid r-1+j \end{cases}$$

for $2 \leq j \leq r$, $S = p-1$, $a_s = s$, $c_{s,j} = t(s)^j$ for $2 \leq j \leq r$ and $d = 1$ in (2.3), we obtain

$$\beta_r + \sum_{s=1}^{p-1} s^{r-1} t(s) + \sum_{j=2}^{r} \frac{1}{r} \binom{r}{j} p^{j-1} \left(\beta_{r+1-j} + \sum_{s=1}^{p-1} s^{r-j} t(s)^{r-j} \right)$$
$$+ \sum_{\substack{j=2 \\ p-1 | r+1-j}}^{r} \frac{1}{r} \binom{r}{j} p^{j-1} \frac{1 - 1/p}{r-j+1} + \frac{p^r}{(r+1)r} = 0.$$

Applying the identity

$$B_r/r = \begin{cases} \beta_r, & p-1 \nmid r \\ \beta_r + \frac{1-1/p}{r}, & p-1 | r \end{cases}$$

to the summations

$$\sum_{j=2}^{r} \frac{1}{r}\binom{r}{j} p^{j-1} \beta_{r+1-j} + \sum_{\substack{j=2 \\ p-1 | r+1-j}}^{r} \frac{1}{r}\binom{r}{j} p^{j-1} \frac{1-1/p}{r-j+1},$$

they become

$$\sum_{j=2}^{r} \frac{1}{r}\binom{r}{j} p^{j-1} \frac{B_{r+1-j}}{r+1-j},$$

and therefore, we have (2.9) $\square$

CHAPTER III

Kummer's congruences of a first kind

In this chapter, we study congruential properties of a given sequence in a different way, mainly, dealing with Hurwitz series. This leads us to another technique regarding Kummer's congruences of a first kind. The technique was invented by Snyder, see [8], based on Carlitz's work. We first give a definition of Hurwitz series and next introduce the operator Ω_p which plays an important role in presenting a useful criterion for Kummer's congruences of a first kind.

3.1 Hurwitz series

Recall that R denotes an integral domain containing $\mathbb{Z}$.

Definition 3.1. *A Hurwitz series (or H-series) $H(x)$ over R is a formal power series of the form*

$$H(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}, a_n \in R.$$

We can easily check that the set of all Hurwitz series over R is an integral domain. The following proposition gives us a basic property of Hurwitz series.

Proposition 3.2. *If $H(x)$ is an H-series defined as above and $a_0 = 0$, then*

$$(H(x))^k \equiv 0 \ (mod\ k!)$$

for all $k \geq 0$.

Proof. Observe that

$$(H(x))^k = k! \left(\sum_{n=k}^{\infty} \sum_{\substack{m_1+m_2+\cdots+m_n=k \\ m_1+2m_2+\cdots+nm_n=n}} \frac{n! a_1^{m_1} a_2^{m_2} \cdots a_n^{m_n}}{(1!)^{m_1} m_1! (2!)^{m_2} m_2! \cdots (n!)^{m_n} m_n!} \right).$$

Then we need to show only

$$\frac{n!}{(1!)^{m_1}m_1!(2!)^{m_2}m_2!\cdots(n!)^{m_n}m_n!} \in \mathbb{Z}$$

where $m_1 + 2m_2 + \cdots + nm_n = n$. Since $m_1 + 2m_2 + \cdots + nm_n = n$, it is obvious that

$$\frac{n!}{m_1!(2m_2)!\cdots(nm_n)!} \in \mathbb{Z},$$

i.e., it suffices to show that

$$\frac{(im_i)!}{(i!)^{m_i}m_i!} \in \mathbb{Z}$$

for all $1 \leq i \leq n$. The proposition follows from the identity

$$\begin{aligned}\frac{(im_i)!}{(i!)^{m_i}m_i!} &= \frac{1}{m_i!}\binom{im_i}{i}\binom{i(m_i-1)}{i}\cdots\binom{i}{i}\\ &= \binom{im_i-1}{i-1}\binom{i(m_i-1)-1}{i-1}\cdots\binom{i-1}{i-1}.\end{aligned}$$

□

3.2 Operator Ω_p

Let D_x be the formal differential operator with respect to x.

Hypothesis. Throughout the rest of this chapter, we will assume the following:

1. $f(x) = \sum_{n=1}^{\infty} c_n \frac{x^n}{n!}$ is an H-series over R with $c_1 = 1$.
2. $D_x f = \sum_{\nu=0}^{\infty} d_\nu f^\nu$ where $d_\nu \in R$ and $d_0 = 1$.

Next, we let p be a fixed prime and define the operator

$$\Omega_p f = (D_x^p - c_p D_x) f,$$

It is clear from the above hypothesis that, for each $r \geq 1$, $\Omega_p^r f$ can be written as a power series in f with coefficients in R. Then, from now on, we express

$$\Omega_p^r f = \sum_{\nu=0}^{\infty} \eta_\nu^{(r)} f^\nu.$$

Some interesting properties concerning Ω_p are listed without proofs, see [2].

Proposition 3.3. *For each positive integer r, we have*

$$\Omega_p^r f = \sum_{m=r}^{\infty} d_{r,m} \frac{x^{m-r}}{(m-r)!},$$

where $d_{r,m} = \sum_{s=0}^{r} (-1)^s \binom{r}{s} c_p^{r-s} c_{n+s(p-1)}$.

Proposition 3.3 allows us to consider the coefficients of $\Omega_p^r f$ instead of the coeffcients of f. Thus, the sequence (c_n) of the coefficients of f satisfies the Kummer's congruence of a first kind if and only if $\Omega_p^r f$ is congruent to 0 modulo p^r for all $r \geq 1$, i.e., the sequence (c_n) satisfies the Kummer's congruence of a first kind if and only if $\eta_\nu^{(r)}$ is congruent to 0 modulo p^r for all $r \geq 1$.

Proposition 3.4. *Let D_x be the differential operator. Then*

$$D_x^{p-1} f - c_p f = b_0 + p \sum_{i=1}^{p-1} b_i f^i + \sum_{\nu=p}^{\infty} b_\nu f^\nu$$

where $b_\mu \in R$ for $\mu \geq 0$.

Corollary 3.5. *Let Ω_p be the operator defined above. Then for each $\nu < p$,*

$$\eta_\nu^{(1)} \equiv 0 \ (mod\ p).$$

3.3 Main theorem

From the remark after Proposition 3.3, our work deals with the coefficients $\eta_\nu^{(r)}$ that seem tough to be determined, especially, for large r. Our main theorem, Theorem 3.14, gives us an efficient criterion to answer the problem. Before we establish the main theorem, the following are needed.

Proposition 3.6. *For each integer z, we define*

$$X(z) = max(0, z)$$

and $e_p(z)$ as the exact exponent of p in the prime decomposition of z. Then

$$\Omega_p^r f \equiv 0 \ (mod\ p^r)$$

if and only if

$$\eta_\nu^{(r)} \equiv 0 \ (mod \ p^{X(r-e_p(\nu!))})$$

for all $\nu \geq 0$.

Proof. Let $(f(x))^\nu = \sum_{m=\nu}^{\infty} c_m^{(\nu)} \frac{x^m}{m!}$. By Proposition 3.2, we have $c_m^{(\nu)} \equiv 0 \ (mod \ \nu!)$. Observe that

$$\begin{aligned} \Omega_p^r f &= \sum_{\nu=0}^{\infty} \eta_\nu^{(r)} f^\nu \\ &= \eta_0^{(r)} + \sum_{\nu=1}^{\infty} \eta_\nu^{(r)} \sum_{m=\nu}^{\infty} c_m^{(\nu)} \frac{x^m}{m!} \\ &= \eta_0^{(r)} + \sum_{m=1}^{\infty} \left(\sum_{\nu=1}^{m} \eta_\nu^{(r)} c_m^{(\nu)} \right) \frac{x^m}{m!}. \end{aligned}$$

If $\eta_\nu^{(r)} \equiv 0 \ (mod \ p^{X(r-e_p(\nu!))})$ for all $\nu \geq 0$, then

$$\eta_0^{(r)} \equiv 0 \ (mod \ p^r)$$

and

$$\eta_\nu^{(r)} c_m^{(\nu)} \equiv 0 \ (mod \ p^{X(r-e_p(\nu!))+e_p(\nu!)})$$

where $\nu \geq 1$. This yields that

$$\eta_\nu^{(r)} c_m^{(\nu)} \equiv 0 \ (mod \ p^r)$$

since $X(r - e_p(\nu!)) + e_p(\nu!) = max(e_p(\nu!), r) \geq r$.

Conversely, suppose that $\Omega_p^r f \equiv 0 \ (mod \ p^r)$. Then

$$\eta_0^{(r)} \equiv 0 \ (mod \ p^r)$$

and

$$\eta_\nu^{(r)} c_m^{(\nu)} \equiv 0 \ (mod \ p^r)$$

where $\nu \geq 1$. If $r > e_p(\nu!)$, then the previous congruence implies

$$\eta_\nu^{(r)} \equiv 0 \ (mod \ p^{r-e_p(\nu!)}).$$

$\square$

Lemma 3.7.

$$\Omega_p^{r+1} f = \Omega_p f \sum_{\nu=0}^{\infty} (\nu+1)\eta_{\nu+1}^{(r)} f^\nu + \sum_{i=1}^{p-1} \binom{p}{i} \sum_{\mu,\nu=1}^{\infty} \eta_{\nu+\mu}^{(r)} f^{\mu-1} D_x^i f^\nu D_x^{p-i} f.$$

Proof. We first establish that, for all $m \in \mathbb{N}$,

$$\Omega_p^{r+1} f = \Omega_p f \left(\sum_{\nu=0}^{m-1} (\nu+1)\eta_{\nu+1}^{(r)} f^\nu + m \sum_{\nu=m}^{\infty} \eta_\nu^{(r)} f^\nu \right) + \sum_{\mu=1}^{m} f^{\mu-1} \sum_{\nu=\mu+1}^{\infty} \eta_\nu^{(r)} \theta(\nu-\mu) + f^m \sum_{\nu=1}^{\infty} \eta_{\nu+m}^{(r)} \Omega_p f^\nu, \tag{3.1}$$

where $\theta(k) = \sum_{i=1}^{p-1} \binom{p}{i} D_x^i f^k D_x^{p-i} f$, for $k \in \mathbb{N}$, by induction on m. For $m = 0$, it follows by the linearity of Ω_p.

Now suppose it is true for m. We will show that it is true for $m+1$. Since

$$\begin{aligned} \Omega_p f^\nu &= D_x^p f^\nu - c_p D_x f^\nu \\ &= \sum_{i=0}^{p} \binom{p}{i} D_x^i f^{\nu-1} D_x^{p-i} f - c_p (f D_x f^{\nu-1} + f^{\nu-1} D_x f) \\ &= f \Omega_p f^{\nu-1} + f^{\nu-1} \Omega_p f + \theta(\nu-1) \end{aligned}$$

for $\nu \geq 1$, we have

$$\begin{aligned} & f^m \sum_{\nu=1}^{\infty} \eta_{\nu+m}^{(r)} \Omega_p f^\nu \\ &= f^m \sum_{\nu=1}^{\infty} \eta_{\nu+m}^{(r)} (f \Omega_p f^{\nu-1} + f^{\nu-1} \Omega_p f + \theta(\nu-1)) \\ &= \Omega_p f \sum_{\nu=0}^{\infty} \eta_{\nu+m+1}^{(r)} f^{\nu+m} + f^m \sum_{\nu=1}^{\infty} \eta_{\nu+m}^{(r)} \theta(\nu-1) + f^{m+1} \sum_{\nu=1}^{\infty} \eta_{\nu+m+1}^{(r)} \Omega_p f^\nu \\ &= \Omega_p f \sum_{\nu=m}^{\infty} \eta_{\nu+1}^{(r)} f^\nu + f^m \sum_{\nu=m+2}^{\infty} \eta_\nu^{(r)} \theta(\nu-m-1) + f^{m+1} \sum_{\nu=1}^{\infty} \eta_{\nu+m+1}^{(r)} \Omega_p f^\nu. \end{aligned}$$

Replace $f^m \sum_{\nu=1}^{\infty} \eta_{\nu+m}^{(r)} \Omega_p f^\nu$ in (3.1) by the previous equation and combine the appropriate terms, we then obtain (3.1) for $m+1$.

Finally, letting m tend to infinity establishes this lemma. □

Proposition 3.8. *Define*

$$\nu_0^{(r)} = \begin{cases} min\{\nu : \eta_\nu^{(r)} \not\equiv 0 \ (mod\ p^r)\} & if \quad \{\nu : \eta_\nu^{(r)} \not\equiv 0 \ (mod\ p^r)\} \neq \phi, \\ \infty & otherwise. \end{cases}$$

and suppose that $\nu_0^{(1)} < p^2$. *Then*

$$\nu_0^{(r)} = \nu_0^{(1)} - (r-1)p$$

for all $r \leq \nu_0^{(r)}/p + 1$.

Proof. We will prove the proposition by induction on r. It is clear for $r = 1$. Now, we assume the proposition for r, i.e. if $r \leq \nu_0^{(1)}/p + 1$ then $\nu_0^{(r)} = \nu_0^{(1)} - (r-1)p$, and then show that $r + 1 \leq \nu_0^{(1)}/p + 1$ implies $\nu_0^{(r+1)} = \nu_0^{(1)} - rp = \nu_0^{(r)} - p$.

By Lemma 3.7,

$$\begin{aligned} \Omega_p^{r+1} f &= \Omega_p f \sum_{\nu=0}^{\infty} (\nu+1)\eta_{\nu+1}^{(r)} f^\nu + \sum_{i=1}^{p-1} \binom{p}{i} \sum_{\mu,\nu=1}^{\infty} \eta_{\nu+\mu}^{(r)} f^{\mu-1} D_x^i f^\nu D_x^{p-i} f. \\ &= \sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} (j+1)\eta_{j+1}^{(r)} \eta_{k-j}^{(1)} \right) f^k + \sum_{i=1}^{p-1} \binom{p}{i} \sum_{\mu,\nu=1}^{\infty} \eta_{\nu+\mu}^{(r)} f^{\mu-1} D_x^i f^\nu D_x^{p-i} f. \end{aligned} \tag{3.2}$$

First, note that for $k \leq \nu_0^{(r)} - p$,

$$\sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} (j+1)\eta_{j+1}^{(r)} \eta_{k-j}^{(1)} \right) f^k \equiv 0 \ (mod\ p^{r+1})$$

since for each $j = 0, 1, 2, \ldots, k+1$ is less than $\nu_0^{(r)}$ implying $\eta_{j+1}^{(r)} \equiv 0 \ (mod\ p^r)$ and $k - j$ is less than $\nu_0^{(1)}$ so $\eta_{k-j}^{(1)} \equiv 0 \ (mod\ p)$.

Consider the second summation of the equation (3.2). Since we can write

$$\sum_{i=1}^{p-1} \binom{p}{i} D_x^i f^\nu D_x^{p-i} f = \sum_{k=X(\nu-p+1)}^{\infty} \delta_k^{(\nu)} f^k$$

where X is defined as in Proposition 3.6, $\delta_k^{(\nu)} \in R$ and $\delta_k^{(\nu)} \equiv 0 \ (mod\ p)$ for all ν and k, a brute force calculation shows that

$$\sum_{i=1}^{p-1} \binom{p}{i} \sum_{\mu,\nu=1}^{\infty} \eta_{\nu+\mu}^{(r)} f^{\mu-1} D_x^i f^\nu D_x^{p-i} f = \sum_{k=0}^{\infty} \alpha_k f^k$$

where

$$\alpha_k = \sum_{\nu=1}^{k+p-1} \sum_{\mu=1}^{k+1-X(\nu-p+1)} \eta_{\nu+\mu}^{(r)} \delta_{k+1-\mu}^{(\nu)}. \tag{3.3}$$

Notice that for each k, $1 \leq \nu \leq k+p-1$ and $1 \leq \mu \leq k+1-X(\nu-p+1)$ imply $\nu+\mu \leq k+p$. Moreover, if $p-1 \leq \nu \leq k+p-1$ and $\mu = k-\nu+p$, then $\nu+\mu = k+p$. Consider the case $k < \nu_0^{(r)} - p$, we have $\alpha_k \equiv 0$ $(mod\ p^{r+1})$ since $\nu+\mu < \nu_0^{(r)}$ and $\delta_{k+1-\mu}^{(\nu)} \equiv 0$ $(mod\ p)$.

Now let $k = \nu_0^{(r)} - p$. Then

$$\alpha_k = \eta_{\nu_0^{(r)}}^{(r)} \sum_{\nu=p-1}^{\nu_0^{(r)}-1} \delta_{\nu-p+1}^{(\nu)} + \sum_{\mu,\nu\geq 1} \eta_{\nu+\mu}^{(r)} \delta_{\nu_0^{(r)}-p+1-\mu}^{(\nu)}.$$

where the second term is the restriction of the summation to those μ and ν with $\nu+\mu < \nu_0^{(r)}$ which vanishes modulo p^{r+1}. By the definition of $\nu_0^{(r)}$, we have $\eta_{\nu_0^{(r)}}^{(r)} \not\equiv 0$ $(mod\ p^r)$. It remains to prove that

$$\sum_{\nu=p-1}^{\nu_0^{(r)}-1} \delta_{\nu-p+1}^{(\nu)} \not\equiv 0\ (mod\ p^2).$$

Since $\nu \geq p-1$,

$$\sum_{i=1}^{p-1} \binom{p}{i} D_x^i f^\nu D_x^{p-i} f = \sum_{k=\nu-p+1}^{\infty} \delta_k^{(\nu)} f^k. \tag{3.4}$$

Observe that $\delta_{\nu-p+1}^{(\nu)}$ only occurs when $i = p-1$ and hence the only contribution to $\delta_{\nu-p+1}^{(\nu)}$ is in the term of

$$\binom{p}{p-1} D_x^{p-1} f^\nu D_x f.$$

Thus $\delta_{\nu-p+1}^{(\nu)} = p\nu(\nu-1)\cdots(\nu-p+2)$ and so

$$\begin{aligned}
\sum_{\nu=p-1}^{\nu_0^{(r)}-1} \delta_{\nu-p+1}^{(\nu)} &= p \sum_{\nu=p-1}^{\nu_0^{(r)}-1} \nu(\nu-1)\cdots(\nu-p+2) \\
&\equiv p \sum_{\substack{\nu=p-1 \\ \nu\equiv -1(p)}}^{\nu_0^{(r)}-1} (p-1)! \\
&\equiv -p \left[\frac{\nu_0^{(r)}}{p} \right]\ (mod\ p^2).
\end{aligned}$$

Since $0 < \nu_0^{(r)} \leq \nu_0^{(1)} < p^2$, we get $\left[\frac{\nu_0^{(r)}}{p}\right] \not\equiv 0 \ (mod\ p)$ and hence

$$\sum_{\nu=p-1}^{\nu_0^{(r)}-1} \delta_{\nu-p+1}^{(\nu)} \not\equiv 0 \ (mod\ p^2).$$

Therefore $\nu_0^{(r+1)} = \nu_0^{(r)} - p$ as required. □

Corollary 3.9. *If there exists $\nu < p^2$ such that $\eta_\nu^{(1)} \not\equiv 0 \ (mod\ p)$, then*

$$\Omega_p^r f \not\equiv 0 \ (mod\ p^r)$$

for some $r \geq 1$.

Proof. By the previous proposition with $r = \nu_0^{(1)}/p + 1$, we obtain $\nu_0^{(r)} = 0$ and hence $\eta_0^{(r)} \not\equiv 0 \ (mod\ p^r)$. The corollary then follows from Proposition 3.6. □

Lemma 3.10. *For each $\nu \geq 1$, we let*

$$\sum_{i=1}^{p-1} \binom{p}{i} D_x^i f^\nu D_x^{p-i} f = \sum_{n=0}^{\infty} \delta_n^{(\nu)} f^n.$$

Then there exist polynomials $p_m(X_1, X_2, \ldots, X_{p-1}) \in p\mathbb{Z}[X_1, X_2, \ldots, X_{p-1}]$ for $m = 1, 2, \ldots, p-1$ independent of ν such that

$$\sum_{i=1}^{p-1} \binom{p}{i} D_x^i f^\nu D_x^{p-i} f = \sum_{m=1}^{p-1} \nu(\nu-1)\cdots(\nu-m+1) f^{\nu-m} p_m(D_x f, D_x^2 f, \ldots, D_x^{p-1} f).$$

Proof. First, we will establish, by induction on i, that

$$D_x^i f^\nu = \sum_{m=1}^{i} \nu(\nu-1)\cdots(\nu-m+1) f^{\nu-m} p_{i,m}(D_x f, D_x^2 f, \ldots, D_x^i f) \qquad (3.5)$$

where $p_{i,m}(X_1, X_2, \ldots, X_i) \in \mathbb{Z}[X_1, X_2, \ldots, X_i]$ and is independent of ν. For $i = 1$, we let $p_{1,1}(X_1) = X_1$.

Now suppose that the equation (3.5) is true for i. Take D_x on both sides of the equation (3.5), we get

$$\begin{aligned}
D_x^{i+1} f^\nu &= \sum_{m=1}^{i} \nu(\nu-1)\cdots(\nu-m+1) D_x \left(f^{\nu-m} p_{i,m}(D_x f, D_x^2 f, \ldots, D_x^i f)\right) \\
&= \sum_{m=1}^{i} \nu(\nu-1)\cdots(\nu-m) f^{\nu-m-1} \left(D_x f\right) p_{i,m}(D_x f, D_x^2 f, \ldots, D_x^i f) \\
&\quad + \sum_{m=1}^{i} \nu(\nu-1)\cdots(\nu-m+1) f^{\nu-m} D_x \left(p_{i,m}(D_x f, D_x^2 f, \ldots, D_x^i f)\right) \\
&= \sum_{m=1}^{i+1} \nu(\nu-1)\cdots(\nu-m+1) f^{\nu-m} p_{i+1,m}(D_x f, D_x^2 f, \ldots, D_x^{i+1} f).
\end{aligned}$$

This follows that

$$\begin{aligned}
&\sum_{i=1}^{p-1} \binom{p}{i} D_x^i f^\nu D_x^{p-i} f \\
&\qquad = \sum_{m=1}^{p-1} \nu(\nu-1)\cdots(\nu-m+1) f^{\nu-m} \sum_{i=1}^{p-1} p_{i,m} \binom{p}{i} (D_x f, \ldots, D_x^i f) D_x^{p-1} f.
\end{aligned}$$

Now take $p_m(X_1, \ldots, X_{p-1}) = \sum_{i=1}^{p-1} p_{i,m} \binom{p}{i} (X_1, \ldots, X_i) X_{p-1}$, we then have the lemma. $\square$

Corollary 3.11. *Let $\delta_n^{(\nu)}$ be defined as above. Then*

$$\delta_n^{(\nu)} \equiv \delta_{n+p}^{(\nu+p)} \ (mod\ p^2).$$

Proof. Let $p_m(D_x f, \ldots, D_x^{p-1} f) = \sum_{k=0}^{\infty} \alpha_{m,k} f^k$. Then we have

$$\begin{aligned}
&\sum_{m=1}^{p-1} \nu(\nu-1)\cdots(\nu-m+1) f^{\nu-m} p_m(D_x f, D_x^2 f, \ldots, D_x^{p-1} f) \\
&\qquad\qquad = \sum_{n=0}^{\infty} \left(\sum_{m=1}^{p-1} \nu(\nu-1)\cdots(\nu-m+1) \alpha_{m,m+n-\nu} \right) f^n
\end{aligned}$$

where $\alpha_{m,k} = 0$ if $k < 0$. Thus

$$\delta_n^{(\nu)} = \sum_{m=1}^{p-1} \nu(\nu-1)\cdots(\nu-m+1) \alpha_{m,m+n-\nu}$$

whereas

$$\delta_{n+p}^{(\nu+p)} = \sum_{m=1}^{p-1} (\nu+p)(\nu+p-1)\cdots(\nu+p-m+1)\alpha_{m,m+n-\nu-p}.$$

We have seen from the proof of the previous lemma that $\alpha_{m,k} \equiv 0$ $(mod\ p)$ for all m and k. This establishes the corollary. $\square$

Proposition 3.12. *If $\eta_\nu^{(1)} \equiv 0$ $(mod\ p)$ for all $\nu < p^e$ where $e > 1$, then*

$$\eta_k^{(r)} \equiv 0\ (mod\ p^{X\left(r-\left[\frac{k}{p^e}\right]\right)})$$

for all $k \geq 0$.

Proof. The proof is done by induction on r. It is apparently shown, by the assumption, for $r = 1$. Now, we assume it true for r and then show it true for $r+1$. To prove this, we let the index $k = qp^e + i$ with $0 \leq i < p^e$ and use induction on $q \geq 0$.

By the equations (3.2), (3.3), and the identity

$$\sum_{\nu=1}^{k+p-1} \sum_{\mu=1}^{k+1-X(\nu-p+1)} \eta_{\nu+\mu}^{(r)} \delta_{k+1-\mu}^{(\nu)} = \sum_{n=2}^{k+p} \eta_n^{(r)} \sum_{\nu=\max(1,n-k-1)}^{n-1} \delta_{k+1-n+\nu}^{(\nu)}$$

for $k \geq 0$, we obtain

$$\eta_k^{(r+1)} = \sum_{j=0}^{k} (j+1)\eta_{j+1}^{(r)} \eta_{k-j}^{(1)} + \sum_{n=2}^{k+p} \eta_n^{(r)} \sum_{\nu=\max(1,n-k-1)}^{n-1} \delta_{\nu-(n-k-1)}^{(\nu)}. \tag{3.6}$$

Now suppose $q = 0$, then $k = i < p^e$. We wish to show that $\eta_k^{(r+1)}$ vanishes modulo p^{r+1}. For the first summation in the equation (3.6), it follows from the hypothesis of the propsition and the induction hypothesis that

$$\sum_{j=0}^{i} (j+1)\eta_{j+1}^{(r)} \eta_{i-j}^{(1)} \equiv 0\ (mod\ p^{r+1}).$$

To deal with the second summation, we first easily have that if $i + p < p^e$, then

$$\sum_{n=2}^{i+p} \eta_n^{(r)} \sum_{\nu=\max(1,n-i-1)}^{n-1} \delta_{\nu-(n-i-1)}^{(\nu)} \equiv 0\ (mod\ p^{r+1}).$$

Next we suppose $p^e - p \leq i < p^e$ which is divided into 2 cases.

Case 1: Suppose $n - i - 1 \geq 1$ and let s be the least residue of i modulo p. Then

$$\begin{aligned}\sum_{n=2}^{i+p} \eta_n^{(r)} \sum_{\nu=n-i-1}^{n-1} \delta_{\nu-(n-i-1)}^{(\nu)} &\equiv \sum_{n=p^e}^{i+p} \eta_n^{(r)} \sum_{\nu=n-i-1}^{n-1} \delta_{\nu-(n-i-1)}^{(\nu)} \\ &= \sum_{n=p^e}^{i+p} \eta_n^{(r)} \sum_{\mu=0}^{i} \delta_\mu^{(n-i-1+\mu)} \ (mod\ p^{r+1}).\end{aligned}$$

By the induction hypothesis, it suffices to show

$$\sum_{\mu=0}^{i} \delta_\mu^{(n-i-1+\mu)} \ (mod\ p^2).$$

Note that Corollary 3.11 implies

$$\begin{aligned}\sum_{\mu=0}^{i} \delta_\mu^{(n-i-1+\mu)} &= \sum_{j=0}^{s} \sum_{\substack{\mu=0 \\ \mu\equiv j(p)}}^{i} \delta_\mu^{(n-i-1+\mu)} + \sum_{j=s+1}^{p-1} \sum_{\substack{\mu=0 \\ \mu\equiv j(p)}}^{i} \delta_\mu^{(n-i-1+\mu)} \\ &\equiv \sum_{j=0}^{s} p^{e-1} \delta_j^{(n-i-1+j)} + \sum_{j=s+1}^{p-1} (p^{e-1} - 1) \delta_j^{(n-i-1+j)} \ (mod\ p^2)\end{aligned}$$

and the first summation in the right-hand side is congruent to 0 modulo p^2. Now, it remains to prove that for each $j \geq s + 1$,

$$\delta_j^{(n-i-1+j)} \equiv 0 \ (mod\ p^2).$$

By Lemma 3.10, we can see that $\delta_j^{(n-i-1+j)}$ is the coefficient of f^j in the expansion with respect to f of

$$\begin{aligned}\sum_{m=1}^{p-1} (n-i-1+j)(n-i-1+j-1) \cdots (n-i-1+j-m+1) \times \\ \times f^{n-i-1+j-m} p_m(D_x f, \ldots, D_x^{p-1} f).\end{aligned}$$

Since $n \geq p^e$ and $j \geq s + 1$, we have

$$n - i - 1 + j \geq n - i + s \geq n + p - p^e \geq p.$$

Moreover, we can see that the only possible contribution to $\delta_j^{(n-i-1+j)}$ occurs when $n - i - 1 + j - m \leq j$ which implies, since $j \leq p - 1$, that

$$n - i - 1 + j - m + 1 \leq n - i + p - 1 - m \leq p.$$

Hence

$$(n-i-1+j)(n-i-1+j-1)\cdots(n-i-1+j-m+1) \equiv 0 \ (mod\ p).$$

Lemma 3.10 gives us $p_m(X_1, X_2, \ldots, X_{p-1}) \in p\mathbb{Z}[X_1, X_2, \ldots, X_{p-1}]$. We obtain the congruence

$$\delta_j^{(n-i-1+j)} \equiv 0 \ (mod\ p^2)$$

as desired.

Case 2: Suppose $n-i-1 < 1$. Then as above

$$\sum_{n=2}^{i+p} \eta_n^{(r)} \sum_{\nu=1}^{n-1} \delta_{\nu-(n-i-1)}^{(\nu)} \equiv \sum_{n=p^e}^{i+p} \eta_n^{(r)} \sum_{\nu=1}^{n-1} \delta_{\nu-(n-i-1)}^{(\nu)} \ (mod\ p^{r+1}).$$

We now consider $p^e \leq n \leq i+p$. Since $n-i-1 < 1$ and $p^e - p \leq i < p^e$, there is exactly one possibility of $n = p^e$ and $i = p^e - 1$. The induction hypothesis for r brings us to show only

$$\sum_{\nu=1}^{p^e-1} \delta_\nu^{(\nu)} \equiv 0 \ (mod\ p^2).$$

Note that

$$\sum_{\nu=1}^{p^e-1} \delta_\nu^{(\nu)} = \sum_{j=1}^{p} \sum_{\substack{\nu=1 \\ \nu \equiv j(p)}}^{p^e-1} \delta_\nu^{(\nu)} \equiv \sum_{j=1}^{p-1} p^{e-1} \delta_j^{(j)} + (p^{e-1}-1)\delta_p^{(p)} \ (mod\ p^2).$$

By Lemma 3.10, it is not hard to see that both terms on the right-hand side in the previous equation are congruent to 0 modulo p^2. We now finish the proof for $q = 0$.

Next, we assume that the proposition holds for $k = qp^e + i$, where $0 \leq i < p^e$. That is,

$$\eta_k^{(r+1)} \equiv 0 \ (mod\ p^{X(r+1-q)}).$$

We wish to show the result holds for $k = (q+1)p^e + i$, i.e.,

$$\eta_k^{(r+1)} \equiv 0 \ (mod\ p^{X(r-q)}).$$

To succeed this, we use the equaion (3.6) to prove that each term on the right-hand side vanishes modulo p^{r-q} where, without loss of generality, we assume $r > q$.

Now fix $k = (q+1)p^e + i$ with $0 \le i < p^e$. Then we have

$$\sum_{j=0}^{k} (j+1)\eta_{j+1}^{(r)}\eta_{k-j}^{(1)} \equiv 0 \ (mod\ p^{r-q}),$$

by the facts that $j < (q+1)p^e$ implies $(j+1)\eta_{j+1}^{(r)} \equiv 0 \ (mod\ p^{r-q})$, $j \ge (q+1)p^e$ implies $(j+1)\eta_{j+1}^{(r)} \equiv 0 \ (mod\ p^{r-q-1})$ and $k - j < i$ implies $\eta_{k-j}^{(1)} \equiv 0 \ (mod\ p)$. Next consider the second term

$$\sum_{n=2}^{k+p} \eta_n^{(r)} \sum_{\nu=\max(1,n-k-1)}^{n-1} \delta_{\nu-(n-k-1)}^{(\nu)}.$$

The induction hypothesis implies that if $i + p < p^e$, then $\eta_n^{(r)} \equiv 0 \ (mod\ p^{r-q-1})$. Since $\delta_{\nu-(n-k-1)}^{(\nu)} \equiv 0 \ (mod\ p)$, the previous expression is congruent to 0 modulo p^{r-q}. Now suppose that $p^e - p \le i < p^e$. Then

$$\sum_{n=2}^{k+p} \eta_n^{(r)} \sum_{\nu=\max(1,n-k-1)}^{n-1} \delta_{\nu-(n-k-1)}^{(\nu)} \equiv \sum_{n=(q+2)p^e}^{k+p} \eta_n^{(r)} \sum_{\nu=\max(1,n-k-1)}^{n-1} \delta_{\nu-(n-k-1)}^{(\nu)} \ (mod\ p^{r-q}). \quad (3.7)$$

As above, the induction hypothesis allows us to show only

$$\sum_{\nu=\max(1,n-k-1)}^{n-1} \delta_{\nu-(n-k-1)}^{(\nu)} \equiv 0 \ (mod\ p^2).$$

The proof is again divided into 2 cases.

Case 1: Suppose $n - i - 1 \ge 1$ and let s be the least residue of i modulo p. Note, by Corollary 3.11, that

$$\begin{aligned}
&\sum_{\nu=n-k-1}^{n-1} \delta_{\nu-(n-k-1)}^{(\nu)} \\
&\quad = \sum_{\mu=0}^{k} \delta_{\mu}^{(n-k-1+\mu)} \\
&\quad = \sum_{j=0}^{s} \sum_{\substack{\mu=0 \\ \mu\equiv j(p)}}^{k} \delta_{\mu}^{(n-k-1+\mu)} + \sum_{j=s+1}^{p-1} \sum_{\substack{\mu=0 \\ \mu\equiv j(p)}}^{k} \delta_{\mu}^{(n-k-1+\mu)} \\
&\quad \equiv \sum_{j=0}^{s} (q+2)p^{e-1}\delta_j^{(n-i-1+j)} + \sum_{j=s+1}^{p-1} ((q+2)p^{e-1} - 1)\delta_j^{(n-i-1+j)} \ (mod\ p^2).
\end{aligned}$$

Clearly, the first summation is congruent to 0 modulo p^2. For the second summation an argument completely analogous to the one for $q = 0$ shows that each $\delta_j^{(n-i-1+j)}$ $(mod\ p^2)$.

Case 2: Suppose $n - k - 1 < 1$. Then as above

$$\sum_{n=2}^{k+p} \eta_n^{(r)} \sum_{\nu=1}^{n-1} \delta_{\nu-(n-k-1)}^{(\nu)} \equiv \sum_{n=(q+2)p^e}^{k+p} \eta_n^{(r)} \sum_{\nu=1}^{n-1} \delta_{\nu-(n-k-1)}^{(\nu)} \ (mod\ p^{r-q}).$$

We now consider $(q+2)p^e \leq n \leq k+p$. Since $n-k-1 < 1$ and $p^e - p \leq i < p^e$, there is exactly one possibility of $n = (q+2)p^e$ and $i = p^e - 1$. The induction hypothesis for r brings us to show only

$$\sum_{\nu=1}^{k} \delta_\nu^{(\nu)} \equiv 0 \ (mod\ p^2).$$

Note that

$$\sum_{\nu=1}^{k} \delta_\nu^{(\nu)} = \sum_{j=1}^{p} \sum_{\substack{\nu=1 \\ \nu \equiv j(p)}}^{k} \delta_\nu^{(\nu)} \equiv \sum_{j=1}^{p-1} (q+2)p^{e-1} \delta_j^{(j)} + ((q+2)p^{e-1} - 1)\delta_p^{(p)} \ (mod\ p^2)$$

that is congruent to 0 modulo p^2, as in case 2 for $q = 0$. Now we complete the proof for $k = (q+1)p^e + i$.

This establishes the induction step and thus the proposition. $\square$

Corollary 3.13. *If $\eta_\nu^{(1)} \equiv 0$ $(mod\ p)$ for all $\nu < p^2$, then*

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} c_p^{r-s} c_{n+s(p-1)} \equiv 0 \ (mod\ p^r),$$

for all $n \geq r \geq 1$.

Proof. Substituting $e = 2$ in Proposition 3.12 gives us

$$\eta_\nu^{(r)} \equiv 0 \ (mod\ p^{X(r-[\frac{\nu}{p^2}])})$$

for all $\nu \geq 0$. Thus since $[\nu/p^2] \leq e_p(\nu!)$,

$$\eta_\nu^{(r)} \equiv 0 \ (mod\ p^{X(r-e_p(\nu!))})$$

for all $\nu \geq 0$. The corollary clearly follows from Proposition 3.3 and Proposition 3.6. $\square$

Now, we are ready to state the main theorem whose proof is straightforward from Corollary 3.9 and Corollary 3.13.

Theorem 3.14. *Let Ω_p and f be defined as above. Then, for $n \geq r \geq 1$,*

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}c_p^{r-s}c_{n+s(p-1)} \equiv 0 \ (mod \ p^r)$$

if and only if

$$\eta_\nu^{(1)} \equiv 0 \ (mod \ p) \ for \ all \ \nu < p^2.$$

Finally, we end up with an example of using Theorem 3.14.

Example 3.15. *Let $f(x) = tan \ x$. Obviously, the Taylor expansion of f about $x = 0$ satisfies the hypothesis. Observe that*

$$f'(x) = sec^2 x$$
$$f''(x) = 2sec^2 x tan \ x$$
$$f'''(x) = 2sec^4 x + 4tan^2 x sec^2 x.$$

Then

$$\begin{aligned}\Omega_3 f &= D_x^3 f - f'''(0)D_x f \\ &= 2sec^4 x + 4tan^2 x sec^2 x - 2sec^2 x \\ &= 2sec^2 x(sec^2 x + 2tan^2 x - 1) \\ &= 6tan^2 x(1 + tan^2 x).\end{aligned}$$

By Theorem 3.14, the sequence $f(0), f'(0), f''(0), \ldots$ satisfies the congruence of the form

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}f^{(p)}(0)^{r-s}f^{(n+s(p-1))}(0) \equiv 0 \ (mod \ p^r)$$

where $n \geq r \geq 1$.

CHAPTER IV

Weak Kummer's congruences of a second kind

We are led to the last type of Kummer's congruence of the form

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}a_p^{r-s}a_{n+sp}\equiv 0\ (mod\ p^r), \tag{4.1}$$

with some additional conditions for n and r, where (a_n) is a sequence in a given setting. It is apparent that the constant sequence $a_n=1$ is one of trivial examples. Moreover, it is valid for all $n,r\geq 0$.

In this chapter, our interest slightly changes to the congruence of the form

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}a_p^{r-s}a_{n+sp}\equiv 0\ (mod\ p^{r_1}), \tag{4.2}$$

where $n,r\geq 0$ and $r_1=[\frac{r+1}{2}]$, having been studied by Carlitz and Stevens, see [5] and [9], respectively. The congruence (4.2) is sometimes said to be a weak Kummer's congruence of a second kind as in [9]. Difference equations and a beautiful technique are here presented.

4.1 Difference equations

Consider the difference equation

$$u_{n+1}^{(k)}=a_0(n)u_n^{(k)}+a_1(n)u_{n-1}^{(k)}+\cdots+a_k(n)u_{n-k}^{(k)} \tag{4.3}$$

of order $k+1$, where $a_j(n)\in\mathbb{Z}[n]$ for $j\geq 0$ ($a_j(n)$ may be added by some additional indeterminates). In addition, we assume that

$$u_0^{(k)}=1 \text{ and } a_j(s)=0\ \ (s=0,1,\ldots,j-1; j=1,2,\ldots,k). \tag{4.4}$$

One property we can show is that u_n satisfies

$$u_nu_m^t-u_{n+tm}\equiv 0\ (mod\ m)$$

for all $n \geq 0$, $m \geq 1$ and $t \geq 1$. It seems natural to ask for the generalization. More precisely, we need to show that

$$\sum_{s=0}^{r}(-1)^s \binom{r}{s} u_m^{t(r-s)} u_{n+stm} \equiv 0 \ (mod \ m^{r_1}),$$

where $n \geq 0, r \geq 0$, $t \geq 1, m \geq 1$ and $r_1 = [\frac{r+1}{2}]$. In order to show this, we replace (4.3) by

$$u_{n+1}^{(k)}(x) = (x + a_0(n))u_n^{(k)}(x) + \sum_{j=1}^{k} a_j(n)u_{n-j}^{(k)}(x) \tag{4.5}$$

where $a_j(n) \in \mathbb{Z}[n]$ for $j \geq 0$. In addition, we assume that

$$u_0^{(k)}(x) = 1 \text{ and } a_j(s) = 0 \ \ (s = 0, 1, \ldots, j-1; j = 1, 2, \ldots, k). \tag{4.6}$$

It is easily seen that $u_n^{(k)}(x)$ are monic polynomials in x of degree n and $u_n^{(k)}(0) = u_n^{(k)}$ for $n \geq 0$.

From now on, we let $u_n^{(k)}(x) = u_n(x)$ for convenience. Our task now is to show that

$$\sum_{s=0}^{r}(-1)^s \binom{r}{s} u_m(x)^{t(r-s)} u_{n+stm}(x) \equiv 0 \ (mod \ m^{r_1}), \tag{4.7}$$

where $n \geq 0, r \geq 0$, $t \geq 1, m \geq 1$ and $r_1 = [\frac{r+1}{2}]$, but first we need some lemmas and have to deal with a number of identities.

Lemma 4.1. *Let $u_n(x)$ be a sequence satisfying* (4.5) *and* (4.6). *Then*

$$u_{n+m}(x) \equiv \ u_n(x)u_m(x) \ (mod \ m)$$

for all $n \geq 0$ and $m \geq 1$.

Proof. We induct on n. It is obvious for $n = 0$. Suppose now that this lemma holds up to the value n. Then

$$\begin{aligned} u_{n+m+1}(x) &= (x + a_0(n+m))u_{n+m}(x) + \sum_{j=1}^{k} a_j(n+m)u_{n+m-j}(x) \\ &\equiv (x + a_0(n))u_{n+m}(x) + \sum_{j=1}^{k} a_j(n)u_{n+m-j}(x) \\ &\equiv (x + a_0(n))u_n(x)u_m(x) + \sum_{j=1}^{k} a_j(n)u_{n-j}(x)u_m(x) \\ &\equiv \left((x + a_0(n))u_n(x) + \sum_{j=1}^{k} a_j(n)u_{n-j}(x) \right) u_m(x) \\ &\equiv u_{n+1}(x)u_m(x) \ (mod\ m) \end{aligned}$$

by the induction hypothesis. □

Corollary 4.2. *Let $u_n(x)$ be a sequence satisfying* (4.5) *and* (4.6)*. Then*

$$u_{n+tm}(x) \equiv u_n(x)u_{tm}(x) \equiv u_n(x)u_m^t(x) \ (mod\ m)$$

for all $n \geq 0$, $m \geq 1$ and $t \geq 1$.

Lemma 4.3. *Let $v_s(x)$ be monic polynomials of degree s with integral coefficients and $m \geq 1$. If there are integers $A_0, A_1, \ldots, A_n$ such that*

$$\sum_{s=0}^{n} A_s v_s(x) \equiv 0 \ (mod\ m), \qquad (4.8)$$

then

$$A_s \equiv 0 \ (mod\ m)$$

for all $0 \leq s \leq n$.

Proof. First, we write

$$v_s(x) = \sum_{j=0}^{s} a_{s,j}x^j$$

where $a_{s,s} = 1$ and $0 \leq s \leq n$. Since

$$\sum_{s=0}^{n} A_s v_s(x) = \sum_{s=0}^{n} A_s \sum_{j=0}^{s} a_{s,j}x^j = \sum_{j=0}^{n} x^j \sum_{s=j}^{n} A_s a_{s,j}$$

and (4.8), we get

$$\sum_{s=j}^{n} A_s a_{s,j} \equiv 0 \ (mod\ m)$$

for $0 \leq j \leq n$. From the fact that $a_{s,s} = 1$ for $0 \leq s \leq n$, the lemma follows by substituting j from n to 0. $\square$

By the equation (4.5),

$$xu_n(x) = u_{n+1}(x) - \sum_{j=0}^{k} a_j(n) u_{n-j}(x)$$

and hence

$$x^s u_n(x) = \sum_{j=-ks}^{s} A_{n,j}(n) u_{n+j}(x),$$

by induction on n, where $A_{n,j}(n) \in \mathbb{Z}[n]$ for $s, n = 0, 1, 2, \ldots$ and in the summation we may assume that $j \geq n$. It follows that

$$u_n(x) u_m^t(x) = \sum_{j=-ktm}^{tm} B_j(n) u_{n+j}(x)$$

where $B_j(n) \in \mathbb{Z}[n]$. Since both sides of the previous equation are polynomials of degree $n + tm$ and the left side is monic, $B_{tm}(n) = 1$, so

$$u_n(x) u_m^t(x) - u_{n+tm}(x) = \sum_{j=-ktm}^{tm-1} B_j(n) u_{n+j}(x). \tag{4.9}$$

By Corollary 4.2, we get

$$\sum_{j=-ktm}^{tm-1} B_j(n) u_{n+j}(x) \equiv 0 \ (mod\ m),$$

and thus

$$B_j(n) \equiv 0 \ (mod\ m) \tag{4.10}$$

for $-ktm \leq j \leq tm - 1$, by Lemma 4.3.

4.2 Operators Δ and δ

Now, for fixed integers m, t, we define the operator Δ by

$$\Delta\varphi_n = u_m^t(x)\varphi_n - \varphi_{n+tm}, \tag{4.11}$$

and more generally,

$$\Delta^r\varphi_n = u_m^t(x)\Delta^{r-1}\varphi_n - \Delta^{r-1}\varphi_{n+tm} \tag{4.12}$$

where $r \geq 1$ and φ_n is an arbitrary function of n. By induction on r, (4.11) and (4.12) imply

$$\Delta^r\varphi_n = \sum_{s=0}^{r}(-1)^s\binom{r}{s}u_m^{t(r-s)}(x)\varphi_{n+stm}. \tag{4.13}$$

Applying Δ^{r-1} to equation (4.9), we obtain

$$\Delta^r u_n(x) = \sum_{j=-ktm}^{tm-1}\Delta^{r-1}\{B_j(n)u_{n+j}(x)\}. \tag{4.14}$$

Define the operator δ by

$$\delta^r\varphi_n = \sum_{s=0}^{r}(-1)^s\binom{r}{s}\varphi_{n+stm}$$

where m and t are fixed. It is clearly equivalent to

$$\varphi_{n+rtm} = \sum_{s=0}^{r}(-1)^s\binom{r}{s}\delta^s\varphi_n.$$

Then, the equation (4.6) becomes

$$\begin{aligned}
&\Delta^r u_n(x)\\
&= \sum_{j=-ktm}^{tm-1}\sum_{s=0}^{r-1}(-1)^s\binom{r-1}{s}u_m^{t(r-1-s)}(x)u_{n+j+stm}(x)B_j(n+stm)\\
&= \sum_{j=-ktm}^{tm-1}\sum_{s=0}^{r-1}(-1)^s\binom{r-1}{s}u_m^{t(r-1-s)}(x)u_{n+j+stm}(x)\sum_{i=0}^{s}(-1)^i\binom{s}{i}\delta^iB_j(n)\\
&= \sum_{j=-ktm}^{tm-1}\sum_{i=0}^{r-1}(-1)^i\delta^iB_j(n)\sum_{s=i}^{r-1}(-1)^s\binom{r-1}{s}\binom{s}{i}u_m^{t(r-1-s)}(x)u_{n+j+stm}(x)\\
&= \sum_{j=-ktm}^{tm-1}\sum_{i=0}^{r-1}(-1)^i\binom{r-1}{i}\delta^iB_j(n)\sum_{s=i}^{r-1}(-1)^s\binom{r-1-i}{s-i}u_m^{t(r-1-s)}(x)u_{n+j+stm}(x)
\end{aligned}$$

$$= \sum_{j=-ktm}^{tm-1} \sum_{i=0}^{r-1} \binom{r-1}{i} \delta^i B_j(n) \sum_{s=0}^{r-1-i} (-1)^s \binom{r-1-i}{s} u_m^{t(r-1-i-s)}(x) u_{n+j+itm+stm}(x)$$

$$= \sum_{j=-ktm}^{tm-1} \sum_{i=0}^{r-1} \binom{r-1}{i} \delta^i B_j(n) \Delta^{r-1-i} u_{n+j+itm}(x). \tag{4.15}$$

Lemma 4.4. *Let $f(n) \in \mathbb{Z}[n]$ and $r \geq 0$. Then*

$$\delta^r f(n) \equiv 0 \ (mod \ m^r).$$

Proof. It suffices to show for the case of $f(n) = n^i$. To see this, we use induction on r. For $r = 1$, we have

$$\delta(n^i) = n^i - (n + tm)^i \equiv 0 \ (mod \ m).$$

Now suppose that the lemma holds for the value r and we want to show for $r + 1$. Note that

$$\begin{aligned}
\delta^{r+1}(n^i) &= \sum_{s=0}^{r+1} (-1)^s \binom{r+1}{s} (n + stm)^i \\
&= n^i + (-1)^{r+1}(n + (r+1)tm)^i + \sum_{s=1}^{r} (-1)^s \left(\binom{r}{s} + \binom{r}{s-1} \right) (n + stm)^i \\
&= \sum_{s=0}^{r} (-1)^s \binom{r}{s} (n + stm)^i + \sum_{s=0}^{r} (-1)^{s+1} \binom{r}{s} (n + (s+1)tm)^i \\
&= \sum_{s=0}^{r} (-1)^s \binom{r}{s} \left((n + stm)^i - (n + stm + tm)^i \right) \\
&= -\sum_{s=0}^{r} (-1)^s \binom{r}{s} \sum_{j=1}^{i} \binom{i}{j} (n + stm)^{i-j} t^j m^j \\
&= -\sum_{j=1}^{i} \binom{i}{j} t^j m^j \sum_{s=0}^{r} (-1)^s \binom{r}{s} (n + stm)^{i-j}.
\end{aligned}$$

The induction hypothesis tells us that

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} (n + stm)^{i-j} \equiv 0 \ (mod \ m^r).$$

This immediately implies the induction step and thus the lemma. ∎

Now, we are ready to establish the main theorem.

4.3 Main theorem

Theorem 4.5. *Let $u_n(x)$ be a sequence satisfying* (4.5) *and* (4.6). *Then*

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}u_m^{t(r-s)}(x)u_{n+stm}(x) \equiv 0 \ (mod\ m^{r_1})$$

for $n \geq 0, r \geq 0$, $t \geq 1, m \geq 1$ and $r_1 = [\frac{r+1}{2}]$.

Proof. We will prove that

$$\Delta^r u_n(x) \equiv 0 \ (mod\ m^{r_1}) \quad (r \geq 1, n \geq 0) \tag{4.16}$$

by induction on r. If $r = 1$, we have $r_1 = 1$ and hence, by Corollary 4.2,

$$\Delta u_n(x) = u_m^t(x)u_n(x) - u_{n+tm}(x) \equiv 0 \ (mod\ m)$$

for $n \geq 0$. Suppose now that (4.16) holds up to $r-1$ for all $n \geq 0$. Consider the equation (4.15), if we view $B_j(n)$ as a polynomial in n, then Lemma 4.4 implies

$$\delta^i B_j(n) \equiv 0 \ (mod\ m^i). \tag{4.17}$$

Next, we use equation (4.15) and set

$$A_i = \delta^i B_j(n)\Delta^{r-1-i}u_{n+j+itm}(x)$$

where $0 \leq i \leq r-1$. From the equations (4.10), (4.17) and the induction hypothesis, we obtain

$$A_0 = B_j(n)\Delta^{r-1}u_{n+j}(x) \equiv 0 \ (mod\ m^{1+[\frac{r}{2}]}),$$
$$A_{r-1} = \delta^{r-1}B_j(n)u_{n+j+(r-1)tm}(x) \equiv 0 \ (mod\ m^{r-1})$$

and

$$A_i \equiv 0 \ (mod\ m^{i+[\frac{r-i}{2}]})$$

where $(1 \leq i \leq r-2)$. It is easily verified that $1 + [\frac{r}{2}]$, $i + [\frac{r-i}{2}]$ and $r-1$ are greater than $r_1 = [\frac{r+1}{2}]$ and thus

$$A_i \equiv 0 \ (mod\ m^{r_1})$$

where $0 \leq i \leq r-1$. This completes the theorem. □

Corollary 4.6. *Let u_n be a sequence satisfying (4.3) and (4.4). Then*

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}u_m^{t(r-s)}u_{n+stm} \equiv 0 \ (mod\ m^{r_1})$$

for $n \geq 0, r \geq 0,\ t \geq 1, m \geq 1$ and $r_1 = [\frac{r+1}{2}]$.

Proof. It follows from the fact that $u_n(0) = u_n$ for all $n \geq 0$. □

Example 4.7. *The Hermite polynomial $H_n(x)$, $n \geq 0$, is defined by*

$$e^{2xt-t^2} = \sum_{n=0}^{\infty} H_n(x)\frac{t^n}{n!} \qquad (H_0(x) = 1).$$

Differentiating with respect to t on both sides of the above equation easily yields the difference equation

$$H_{n+1}(x) = 2xH_n(x) - 2nH_{n-1}(x).$$

By Corollary 4.6, we obtain

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}H_m^{t(r-s)}(x)H_{n+stm}(x) \equiv 0 \ (mod\ m^{r_1})$$

for $n \geq 0, r \geq 0,\ t \geq 1, m \geq 1$.

CHAPTER V

Relationships among three types of Kummer's congruences

In the previous three chapters, we have mentioned each type of Kummer's congruence as well as each used technique, basically, starting with a nice setup and an appropriate operator. However, they are quite unique. Another interesting aspect is to investigate some relationships among them.

5.1 The zeroth and the first kinds

As seen in Definition 1.1, we are not restricted by the conditions of parameters n and r. However, a Kummer's congruence of a zeroth kind of the form

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}a_{n+s(p-1)} \equiv 0 \ (mod\ p^r) \tag{5.1}$$

and a Kummer's congruence of a first kind of the form

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}a_p^{r-s}a_{n+s(p-1)} \equiv 0 \ (mod\ p^r), \tag{5.2}$$

where (a_n) is a sequence in R and $n \geq r \geq 1$, have often appeared in several papers, see [4], [8] and [9].

A little fact regarding both of them is given below.

Proposition 5.1. *Let (a_n) be a sequence in R and $a_p \equiv 1\ (mod\ p)$. If (a_n) satisfies the congruence (5.1), then (a_n) also satisfies the congruence (5.2). Moreover, the converse is true.*

Proof. We first show that the congruence (5.1) implies the congruence (5.2). Suppose the congruence (5.1) holds for all $n \geq r \geq 1$. By the assumption, we have

$a_p = 1 + kp$ for some $k \in R$. Hence, for each $n \geq r \geq 1$,

$$\begin{aligned}\sum_{s=0}^{r}(-1)^s\binom{r}{s}a_p^{r-s}a_{n+sp} &= \sum_{s=0}^{r}(-1)^s\binom{r}{s}a_{n+sp}(1+kp)^{r-s}\\ &= \sum_{s=0}^{r}(-1)^s\binom{r}{s}a_{n+sp}\sum_{j=0}^{r-s}\binom{r-s}{j}k^jp^j\\ &= \sum_{j=0}^{r}\binom{r}{j}k^jp^j\sum_{s=0}^{r-j}(-1)^s\binom{r-j}{r-s-j}a_{n+sp}.\end{aligned}$$

But

$$\sum_{s=0}^{r-j}(-1)^s\binom{r-j}{r-s-j}a_{n+sp} = \sum_{s=0}^{r-j}(-1)^s\binom{r-j}{s}a_{n+sp} \equiv 0 \ (mod\ p^{r-j}).$$

The converse implication can be proved in a similar way. □

5.2 The zeroth and the second kinds

Let $\beta_1, \beta_2, \ldots$ be a sequence with $\beta_1 = 1$ satisfying, for $r \geq 2$,

$$\beta_r + \sum_{j=2}^{r} f_{j-1}(r)\frac{p^{j-1}}{j!}\beta_{r+1-j} + \sum_{j=1}^{r} g_{j-1}(r)\frac{p^{j-1}}{j!}\sum_{s=1}^{S} c_{s,j}a_s^{r-j} + \sum_{j=2}^{r} h_{j-2}(r)\frac{p^{j-2}}{j!} + d\frac{p^r}{(r+1)r} = 0$$

where k is fixed, $f_{j-1}(r) \in \mathbb{Z}[r]$ have degree $\leq j-1$ with $f_{j-1}(r) \equiv 0 \ (mod\ j!)$ for $2 \leq j \leq k$, $f_{j-1}(r) = 0$ for $j > k$, $g_{j-1}(r) = h_{j-2}(r) = 0$ for $j \geq 2$, $g_0(r) = 0$ and $d = 0$. This reduces to

$$\beta_r + \sum_{j=2}^{r} f_{j-1}(r)\frac{p^{j-1}}{j!}\beta_{r+1-j} = 0, \tag{5.3}$$

where $f_{j-1}(r) \in \mathbb{Z}[r]$ have degree $\leq j-1$ with $f_{j-1}(r) \equiv 0 \ (mod\ j!)$ for $2 \leq j \leq k$, $f_{j-1}(r) = 0$ for $j > k$.

We have already known from Theorem 2.5 that the sequence (β_r) satisfies the congruence

$$\sum_{t=0}^{n}(-1)^{n-t}\binom{n}{t}\beta_{k+(i+t)(p-1)} \equiv 0 \ (mod\ p^n)$$

where $n \leq p-3$, $k > n \geq 1$ and $i \geq 0$.

The following proposition reveals another view of β_r.

Proposition 5.2. *Let β_r be defined in* (5.3) *and $u_1, u_2, \ldots$ a sequence satisfying the difference equation*

$$u_{r+1} = a_1(r)u_r + a_2(r)u_{r-1} + \cdots + a_{k-1}(r)u_{r-k+2} \quad (r \geq 1) \tag{5.4}$$

of order $k-1$, where $a_j(r) = -f_j(r)\frac{p^j}{(j+1)!}$ for $1 \leq j \leq k-1$. If we assume that

$$u_1 = 1 \text{ and } f_j(s) = 0 \quad (s = 1, 2, \ldots, j-1; j = 2, 3, \ldots, k-1), \tag{5.5}$$

then $u_r = \beta_r$ for all $r \geq 1$.

Proof. It suffices to verify that $u_r = \beta_r$ for all $1 \leq r \leq k-1$. Obviously, $u_1 = \beta_1$. Now, let $r \geq 2$ and suppose that $u_i = \beta_i$ for $1 \leq i \leq r-1 < k-1$. To show $u_r = \beta_r$, we observe that, by (5.5),

$$\begin{aligned} u_r &= a_1(r-1)u_{r-1} + a_2(r-1)u_{r-2} + \cdots + a_{r-1}(r-1)u_1 \\ &= -f_1(r-1)\frac{p}{2!}u_{r-1} - f_2(r-1)\frac{p^2}{3!}u_{r-2} - \cdots - f_{r-1}(r-1)\frac{p^{r-1}}{r!}u_1 \\ &= -\sum_{j=2}^{r} f_{j-1}(r-1)\frac{p^{j-1}}{j!}u_{r+1-j}. \end{aligned}$$

The induction hypothesis yields $u_{r+1-j} = \beta_{r+1-j}$ for all $2 \leq j \leq r$. Thus

$$u_r = -\sum_{j=2}^{r} f_{j-1}(r-1)\frac{p^{j-1}}{j!}\beta_{r+1-j} = \beta_r.$$

□

Corollary 5.3. *The sequence β_r defined in* (5.3) *satisfies the congruence of the form*

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}\beta_{m+1}^{t(r-s)}\beta_{n+stm+1} \equiv 0 \ (mod\ m^{r_1})$$

where $n \geq 0, r \geq 0$, $t \geq 1, m \geq 1$ and $r_1 = [\frac{r+1}{2}]$.

Proof. The previous proposition tells us that β_r satisfies equations (4.3) and (4.4) mentioned in Chapter IV. □

REFERENCES

[1] Bachmann, G.: Introduction to p-adic numbers and valuation theory, *Academic Press Inc.*, 1964.

[2] Carlitz, L.: Congruences for the coefficients of the Jacobi elliptic functions, *Duke Math. J.*, **16**(1949), 297-302.

[3] Carlitz, L.: Some theorems on Kummer's congruences, *Duke Math. J.*, **20**(1953), 423-431.

[4] Carlitz, L.: Criteria for Kummer's congruences, *Acta Arith.*, **6**(1961), 375-391.

[5] Carlitz, L.: Congruence properties of certain linear homogeneous difference equations, *Acta Arith.*, **7**(1962), 173-186.

[6] Johnson, W.: p-adic proofs of congruences for the Bernoulli numbers, *Advanced in Math.*, (1992), 251-265.

[7] Kummer, E.: Über eine allgemeine Eigenschaft der rationalen Entwicklungskoefficienten einer bestimmten Gattung analytischer Funktionen, *J. reine angew. Math.*, **41**(1851), 368-372.

[8] Snyder, C.: Kummer congruences for the coefficients of Hurwitz series, *Acta Arith.*, **40**(1982), 175-191.

[9] Stevens, H.: Kummer's congruences of a second kind, *Math. Zeitschr.*, **79**(1962), 180-192.

VITA

Mr. Supreedee Dangskul was born in Bangkok, Thailand. In 2004, he gratuated with a Bachelor of Science in Mathematics from Kasetsart University and, a year later, decided to join the M.Sc. program at Chulalongkorn University.