Acta Math. Univ. Comenianae
Vol. LXXIX, 1(2010), pp. 135–142

THE INVERSE OF THE PASCAL LOWER TRIANGULAR MATRIX MODULO p

A. IMANI and A. R. MOGHADDAMFAR

Abstract. Let $L(n)_p$ be the Pascal lower triangular matrix with coefficients $\binom{i}{j} \pmod p, 0 \leq i,j < n$. In this paper, we found the inverse of $L(n)_p$ modulo p. In fact, we generalize a result due to David Callan [**4**].

1. Introduction

Consider the infinite unipotent lower triangular matrix

$$L(\infty) = \begin{pmatrix} 1 & & & & \\ 1 & 1 & & & \\ 1 & 2 & 1 & & \\ 1 & 3 & 3 & 1 & \\ \vdots & & & & \ddots \end{pmatrix} = \exp \begin{pmatrix} 0 & & & & & \\ 1 & 0 & & & & \\ 0 & 2 & 0 & & & \\ & 0 & 3 & 0 & & \\ & & & & & \ddots \end{pmatrix}$$

with coefficients $L(\infty)_{i,j} = \binom{i}{j}$, $i,j \geq 0$, where, as usual, we use the convention $\binom{i}{j} = 0$ if $i < j$. We denote by $L(n)$ the $n \times n$ principal submatrix with coefficients $L(n)_{i,j}$, $0 \leq i,j < n$ obtained by considering the first n rows and columns of $L(\infty)$. Given a prime p, we define $L(n)_p$ with coefficients $(L(n)_p)_{i,j} \in \{0,1,\ldots,p-1\}$ as the reduction modulo p of $L(n)$ by setting

$$(L(n)_p)_{i,j} = \binom{i}{j} \pmod p \in \{0,1,\ldots,p-1\}.$$

For instance, the matrices $L(5)_2$, $L(6)_3$ and $L(7)_5$ are given as follows:

$$L(4)_2 = \begin{pmatrix} 1 & & & & \\ 1 & 1 & & & \\ 1 & 0 & 1 & & \\ 1 & 1 & 1 & 1 & \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad L(5)_3 = \begin{pmatrix} 1 & & & & & \\ 1 & 1 & & & & \\ 1 & 2 & 1 & & & \\ 1 & 0 & 0 & 1 & & \\ 1 & 1 & 0 & 1 & 1 & \\ 1 & 2 & 1 & 1 & 2 & 1 \end{pmatrix}$$

Received June 6, 2009; revised July 27, 2009.
2000 *Mathematics Subject Classification.* Primary 15A09, 15A36, 11C20.
Key words and phrases. Pascal matrix modulo p; inverse matrix; Thue-Morse sequence.

$$L(6)_5 = \begin{pmatrix} 1 & & & & & & \\ 1 & 1 & & & & & \\ 1 & 2 & 1 & & & & \\ 1 & 3 & 3 & 1 & & & \\ 1 & 4 & 1 & 4 & 1 & & \\ 1 & 0 & 0 & 0 & 0 & 1 & \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

For a prime p and a positive integer n, we denote by $s_p(n)$ the sum of the digits in the base-p representation of the integer n, that is, $s_p(n) = \sum_{k\geq 0} n_k$ when writing $n = \sum_{k\geq 0} n_k p^k$ in base p. The *Thue-Morse sequence*

$$\mathbf{t} = \Big\{t(n) = s_2(n) \pmod 2\Big\}_{n=0}^{\infty} = 0\,1\,1\,0\,1\,0\,0\,1\,1\,0\,0\,1\,0\,1\,1\,0\ldots,$$

records the parity of the sum of the binary digits of $n = \sum_{k\geq 0} n_k 2^k$. It can also be defined recursively by $t(0) = 0$, $t(2n) = t(n)$, $t(2n+1) = \overline{t(n)}$, for all $n \geq 0$, where, for $x \in \{0, 1\}$, we define $\overline{x} = 1-x$. The sequence $\mathbf{t}$ has appeared in various fields of mathematics, see, for instance, [**1**]. Replacing 0 by a and 1 by b yields the Thue-Morse sequence on the alphabet $\mathcal{A} = \{a, b\}$ (called the ± 1 Thue-Morse sequence if $a = 1$ and $b = -1$)

$$\mathbf{t}(a, b) = a\ b\ b\ a\ b\ a\ a\ b\ b\ a\ a\ b\ a\ b\ b\ a\ \ldots$$

In [**4**], David Callan showed that the sequence $\mathbf{t}$ is related to the matrix $L(\infty)_2$. In fact, the following result is due to Callan.

Callan Theorem ([**4**])**.** *The inverse matrix of $L(\infty)_2$ is a $(0, \pm 1)$-matrix. It has the same pattern of zeroes as $L(\infty)_2$ and the nonzero entries in each column form the ± 1 Thue-Morse sequence.*

In order to prove his result, Callan defined the lower triangular matrix $L_2(x)$ with entries $L_2(x)_{i,j}$ by

$$L_2(x)_{i,j} = \binom{i}{j} x^{s_2(i-j)} \pmod 2 \qquad \text{for each } i, j \geq 0,$$

and then he showed that $L_2(x) + L_2(y) = L_2(x + y)$. It is worth mentioning that, Roland Bacher and Robin Chapman have obtained the same result observing that the $2^k \times 2^k$ upper left submatrix of $L_2(x)$ is the k-fold Kronecker product of $\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$ (see [**2**], [**3**]). Here, we are going to generalize Callan Theorem. Following Callan [**4**], we present the following definition.

Definition 1. Let x be an indeterminate. Define the infinite lower triangular matrix $L_p(x)$ with coefficients $L_p(x)_{i,j}$ by setting

$$L_p(x)_{i,j} = \binom{i}{j} x^{s_p(i-j)} \pmod p.$$

In particular, we have $L_p(1) = L(\infty)_p$.

Then the matrices $L_2(x)$ and $L_3(x)$, for example, are given by

$$L_2(x) = \begin{pmatrix} 1 & & & & & & & & \\ x & 1 & & & & & & & \\ x & 0 & 1 & & & & & & \\ x^2 & x & x & 1 & & & & & \\ x & 0 & 0 & 0 & 1 & & & & \\ x^2 & x & 0 & 0 & x & 1 & & & \\ x^2 & 0 & x & 0 & x & 0 & 1 & & \\ x^3 & x^2 & x^2 & x & x^2 & x & x & 1 & \\ \vdots & & & & & & & & \ddots \end{pmatrix}$$

and

$$L_3(x) = \begin{pmatrix} 1 & & & & & & & & \\ x & 1 & & & & & & & \\ x^2 & 2x & 1 & & & & & & \\ x & 0 & 0 & 1 & & & & & \\ x^2 & x & 0 & x & 1 & & & & \\ x^3 & 2x^2 & x & x^2 & 2x & 1 & & & \\ x^2 & 0 & 0 & 2x & 0 & 0 & 1 & & \\ x^3 & x^2 & 0 & 2x^2 & 2x & 0 & x & 1 & \\ \vdots & & & & & & & & \ddots \end{pmatrix}.$$

Indeed, the purpose of this paper is to prove the following theorem.

Main Theorem. *Let p be a prime and let x and y be indeterminates. Then there holds*

$$L_p(x) \cdot L_p(y) \equiv L_p(x+y) \pmod p. \tag{1}$$

In particular, we conclude that $L_p(1)^{-1} \equiv L_p(-1) \pmod p$.

It is worth mentioning that the idea in the proof of this Theorem follows that one of Callan [**4**].

As an immediate consequence of Main Theorem, we have the following.

Corollary 1. If n is a positive integer, then we have $L_p(x)^n \equiv L_p(nx) \pmod p$.

Proof. By an easy induction on n. □

Corollary 2. If r is a rational number, then we have $L_p(r) \equiv L_p(1)^r \pmod p$.

Proof. Let $r = \frac{m}{n}$, with m, n positive integers. Then, by Corollary 1, we obtain

$$L_p(r)^n \equiv L_p\left(\frac{m}{n}\right)^n \equiv L_p(m) \equiv L_p(1)^m \pmod p.$$

For negative r, it now suffices to show that $L_p(1)^{-1} \equiv L_p(-1) \pmod p$, and this follows

$$L_p(-1)L_p(1) \equiv L_p(-1+1) \equiv L_p(0) \equiv I \pmod p,$$

by Main Theorem. This completes the proof of the corollary. □

Remark 1. Note that the main result of this paper can also be obtained by the Kronecker product method attributed to Roland Bacher: the $p^k \times p^k$ upper left submatrix of $L_p(x)$ is the k-fold Kronecker product of the upper left $p \times p$ submatrix of $L_p(x)$.

2. Preliminaries

In this section, we collect a number of results that we will need in the proof of the Main theorem. We start with a well-known result due to Lucas. In fact, Lucas discovered an easy method to determine the value of $\binom{n}{m} \pmod p$.

Lemma 1 (Lucas Theorem [**5**])**.** *Let p be a prime number and m, n be non-negative integers. Suppose*

$$m = \sum_{k\geq 0} m_k p^k \qquad \textit{and} \qquad n = \sum_{k\geq 0} n_k p^k,$$

are written in base p, that is, $m_k, n_k \in \{0, 1, \ldots, p-1\}$ for all k. Then we have

$$\binom{n}{m} \equiv \binom{n_0}{m_0}\binom{n_1}{m_1}\cdots\binom{n_d}{m_d} \pmod p.$$

In 1852 Kummer showed that the power of prime p that divides the binomial coefficient $\binom{i}{j}$ is given by the number of 'carries' when we add j and $i-j$ in base p.

Lemma 2 (Kummer Theorem [**6**])**.** *If p is a prime number, then its exponent in the canonical expansion of the binomial coefficient $\binom{i}{j}$ into prime factors is equal to the number of carries required when adding the numbers j and $i - j$ in base p.*

Proof. Note that the identity

$$\binom{i}{j} = \frac{i!}{j!(i-j)!}$$

implies that

$$e_p\left(\binom{i}{j}\right) = e_p(i!) - e_p(j!) - e_p((i-j)!),$$

where $e_p(k)$ is the exponent of p in the prime factorization of k. It is not difficult to see that

$$e_p(k!) = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \cdots,$$

because among the numbers $1, 2, \ldots, k$, there are exactly $\lfloor \frac{k}{p} \rfloor$ numbers divisible by p, exactly $\lfloor \frac{k}{p^2} \rfloor$ numbers divisible by p^2, and so on. Thus,

$$e_p\Big(\binom{i}{j}\Big) = \sum_{l\geq 0} \Big(\Big\lfloor \frac{i}{p^l} \Big\rfloor - \Big\lfloor \frac{j}{p^l} \Big\rfloor - \Big\lfloor \frac{i-j}{p^l} \Big\rfloor\Big).$$

Now, it suffices to note that in this sum, the lth summand is either 1 or 0 depending on whether or not there is a carry from the $(l-1)$th digit. $\square$

Definition 2. Let p be a prime and i, j be non-negative integers. Suppose

$$i = \sum_{k \geq 0} i_k p^k \qquad \text{and} \qquad j = \sum_{k \geq 0} j_k p^k,$$

are written in base p. We say i is *p-free of j* if

$$0 \leq i_k + j_k \leq p - 1, \quad \text{for all } k.$$

Lemma 3. *Let p be a prime number and let i and j be positive integers with $i \geq j$. Suppose that $i = \sum_{k \geq 0} i_k p^k$ and $j = \sum_{k \geq 0} j_k p^k$ are written in base p. Then, the following four statements are equivalent:*

(a) *$i - j$ is p-free of j.*
(b) *for every $k \geq 0$, $i_k \geq j_k$.*
(c) *There exists l between i and j such that $i - l$ is p-free of l and $l - j$ is p-free of j.*
(d) $0 \not\equiv \binom{i}{j} \pmod{p}$.

Proof. Before starting the proof we give an easy observation

$$(i - j)_k = \begin{cases} i_k - j_k & \text{if} \quad i_k \geq j_k \\ p + i_k - j_k & \text{if} \quad i_k < j_k. \end{cases} \tag{2}$$

$(a) \Rightarrow (b)$ Assume the contrary that there exists k such that $i_k < j_k$. But then, by Eq. (2), we have

$$(i - j)_k + j_k = p + i_k - j_k + j_k = p + i_k > p - 1,$$

which contradicts our assumption, i.e., $i - j$ is p-free of j.

$(b) \Rightarrow (a)$ We can easily see that

$$(i - j)_k + j_k = i_k - j_k + j_k = i_k \leq p - 1,$$

and so by definition, we conclude the result.

$(a) \Rightarrow (c)$ If $i - j$ is p-free of j, then by part (b), we have $i_k \geq j_k$ for every k. Now, for every k, we choose l_k such that $i_k \geq l_k \geq j_k$, and we put $l = \sum_{k \geq 0} l_k p^k$. It is evident that $j \leq l \leq i$. Moreover, by Eq. (2), we observe that

$$(i - l)_k + l_k = i_k - l_k + l_k = i_k \leq p - 1,$$

and also

$$(l - j)_k + j_k = l_k - j_k + j_k = l_k \leq i_k \leq p - 1$$

which implies that $i - l$ is p-free of l and $l - j$ is p-free of j by definition.

$(c) \Rightarrow (a)$ Assume that there exists $j \leq l \leq i$ such that $i - l$ is p-free of l and $l - j$ is p-free of j. Put $l = \sum_{k \geq 0} l_k p^k$, where $l_k \in \{0, 1, \ldots, p - 1\}$. Then, by part (a), we obtain $j_k \leq l_k \leq i_k$ for every k. Now, by Eq. (2), it follows that

$$(i - j)_k + j_k = i_k - j_k + j_k = i_k \leq p - 1,$$

and so $i - j$ is p-free of j by definition.

$(d) \Leftrightarrow (a)$ This follows immediately from Kummer Theorem.

This completes the proof of the lemma. $\square$

Remark 2. Note that, if $i \geq j$ and $i-j$ is p-free of j, then we have $s_p(i-j) = s_p(i) - s_p(j)$.

Lemma 4. *Let p be a prime and n, r be positive integers. Then we have*

$$\sum_{\substack{0 \leq t \leq n \\ s_p(t)=r}} \binom{n}{t} \equiv \binom{s_p(n)}{r} \pmod{p}.$$

Proof. We write $n = \sum_{k=0}^{d} n_k p^k$ in base p, so that $0 \leq n_k \leq p-1$ for each k. Now, we consider the following equation

$$(1+X)^{s_p(n)} = (1+X)^{n_0}(1+X)^{n_1} \cdots (1+X)^{n_d} \tag{3}$$

and compare the coefficient of X^r modulo p in both sides of this equation. Evidently, the coefficient of X^r on the left-hand side of Eq. (3) is equal to $\binom{s_p(n)}{r} \pmod{p}$. On the other hand, the coefficient of X^r on the right-hand side of Eq. (3) is equal to

$$\sum_{r_0+r_1+\cdots+r_d=r} \binom{n_0}{r_0}\binom{n_1}{r_1} \cdots \binom{n_d}{r_d} \pmod{p}. \tag{4}$$

But, by Lucas Theorem, the sum in Eq. (4) is congruent to

$$\sum_{\substack{0 \leq t \leq n \\ s_p(t)=r}} \binom{n}{t} \pmod{p}.$$

This completes the proof of the lemma. □

3. Proof of the Main Theorem

Proof. For the proof of the Eq. (1) we compute the (i,j)-th entry of $L_p(x) \cdot L_p(y)$, that is,

$$(L_p(x) \cdot L_p(y))_{i,j} = \sum_t L_p(x)_{i,t} L_p(y)_{t,j}.$$

First of all, since the matrices $L_p(x)$ and $L_p(y)$ are lower triangular matrices, thus $L_p(x) \cdot L_p(y)$ is also a lower triangular matrix. Furthermore, it is easy to see the product of row i of $L_p(x)$ with column i of $L_p(y)$ is always 1, since every pair of entries except entry i is either 0 in the row or 0 in the column, and the product at entry i is $1 \times 1 = 1$ for $i \geq 1$. Now, we must show that the product of row i of $L_p(x)$ with column j of $L_p(y)$ when $i > j$ is always $L_p(x+y)_{i,j}$. Therefore, from now on we assume that $i > j$. In this case, the (i,j)-th entry of $L_p(x) \cdot L_p(y)$ is equal to

$$(L_p(x) \cdot L_p(y))_{i,j} = \sum_{t=j}^{i} L_p(x)_{i,t} L_p(y)_{t,j}.$$

We now consider two cases separately:

Case 1. *$i-j$ is not p-free of j.*

In this case, by Lemma 3, there does not exist t between j and i such that $i-t$ is p-free of t and $t-j$ is p-free of j. Hence for every t between j and i, we have $L_p(x)_{i,t}=0$ or $L_p(y)_{t,j}=0$, and so

$$(L_p(x)\cdot L_p(y))_{i,j}=\sum_{t=j}^{i}0=0=L_p(x+y)_{i,j}.$$

Case 2. *$i-j$ is p-free of j.*

In this case, by Lemma 4, we have $\binom{i}{j} \pmod p \not\equiv 0$. First, we notice that

$$\binom{i}{t}\binom{t}{j}=\binom{i}{j}\binom{i-j}{t-j},\qquad \text{for } i\geq t\geq j. \tag{5}$$

Now, we calculate the sum in question

$$\begin{aligned}
(L_p(x)\cdot L_p(y))_{i,j} &\equiv \sum_{t=j}^{i}\binom{i}{t}\binom{t}{j}x^{s_p(i-t)}y^{s_p(t-j)} \pmod p\\
&\equiv \sum_{t=j}^{i}\binom{i}{j}\binom{i-j}{t-j}x^{s_p(i-t)}y^{s_p(t-j)} \pmod p \qquad \text{(by Eq. (5))}\\
&= \sum_{t=0}^{i-j}\binom{i}{j}\binom{i-j}{t}x^{s_p(i-j-t)}y^{s_p(t)} \pmod p
\end{aligned}$$

If $i-j-t$ is not p-free of t, then, by Lemma 3, we obtain that $0\equiv\binom{i-j}{t} \pmod p$. Hence, we may restrict the last sum to $0\leq t\leq i-j$ such that $i-j-t$ is p-free of t. But then, by Remark 2, we have $s_p(i-j-t)=s_p(i-j)-s_p(t)$. Thus we obtain

$$\begin{aligned}
(L_p(x)\cdot L_p(y))_{i,j} &= \binom{i}{j}\sum_{t=0}^{i-j}\binom{i-j}{t}x^{s_p(i-j)-s_p(t)}y^{s_p(t)} \pmod p\\
&= \binom{i}{j}\sum_{r=0}^{s_p(i-j)}\Big\{\Big(\sum_{\substack{0\leq t\leq i-j\\ s_p(t)=r}}\binom{i-j}{t}\Big)x^{s_p(i-j)-r}y^r\Big\} \pmod p\\
&\equiv \binom{i}{j}\sum_{r=0}^{s_p(i-j)}\binom{s_p(i-j)}{r}_p x^{s_p(i-j)-r}y^r \pmod p \quad \text{(by Lemma 4)}\\
&= \binom{i}{j}(x+y)^{s_p(i-j)} \pmod p\\
&= L_p(x+y)_{i,j}
\end{aligned}$$

as desired. ∎

References

1. Allouche J. P. and Shallit J., *The ubiquitous Prouhet-Thue-Morse sequence*, Sequences and their applications (Singapore, 1998), 1–16, Springer Ser. Discrete Math. Theor. Comput. Sci., Speringer, London, 1999.

2. Bacher R. and Chapman R., *Symmetric Pascal matrices modulo p*, European J. Combinatorics, **25** (2004), 459–473.

3. Bacher R., *La suite de Thue-Morse et la catégorie Rec*, Comptes Rendues Acad. Sci. Paris, Ser. I, **342** (2006), 161–164.

4. Callan D., *Sierpinski's triangle and the Prouhet-Thue-Morse word*, arXiv:math/0610932v3 [math.CO], 18 Nov. 2006.

5. Graham R. L., Knuth D. E. and Patashnik O., *Concrete mathematics*, second edition, Addison-Wesley, 1994.

6. Kummer E. E., *Über die Ergänzungätze zu den allgemeinen Reciprocitatsgesetzen*, J. Reine Angew. Math. **44** (1852), 93–146.

A. Imani, Department of Mathematics, Faculty of Science, K. N. Toosi University of Technology, P. O. Box 16315–1618, Tehran, Iran

A. R. Moghaddamfar, Department of Mathematics, Faculty of Science, K. N. Toosi University of Technology, P. O. Box 16315–1618, Tehran, Iran, *e-mail*: `moghadam@kntu.ac.ir`