ON A CLASS OF CONGRUENCES

FOR LUCAS SEQUENCES

Paul Thomas Young

Department of Mathematics, University of Charleston
Charleston, SC 29424

1. INTRODUCTION

Let $\lambda, \mu \in \mathbb{Z}$ and define a sequence of integers $\{H_n(\lambda, \mu)\}_{n \geq 0}$ by the binary linear recurrence

$$H_0(\lambda, \mu) = 2,\ H_1(\lambda, \mu) = \lambda, \text{ and } H_{n+1}(\lambda, \mu) = \lambda H_n(\lambda, \mu) + \mu H_{n-1}(\lambda, \mu) \text{ for } n > 0. \tag{1.1}$$

The objects of study in this article are systems of congruences

$$H_{mp^r}(\lambda, \mu) \equiv B \pmod{p^{r+1}\mathbb{Z}} \tag{1.2}$$

for nonnegative integers r, where p is a prime and m, B are integers. Such congruences were conjectured by P. Filipponi [2] in the case $B = m = \lambda = 1$, $\mu = p - 1$ for primes $p \geq 5$, and subsequently proved by R. André-Jeannin [1] whose proof, based on a method of E. Lucas, applied also for $\mu \equiv 0, -1 \pmod{p}$. In this article we use the methods of [4] to show that every sequence $\{H_n(\lambda, \mu)\}$ exhibits at least one such system of congruences for every prime p, and to give complete characterizations of these congruences (see §3). Our approach uses the elementary theory of finite and p-adic fields; the reader is referred to [3] for a detailed exposition of these topics. We begin with the following existence theorem.

Theorem 1. (i). *Suppose that for some integers λ, μ there exists a prime p, integers m, A, B with $m, A > 0$ and $(A, B) = 1$, and a function $f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$ satisfying $\lim_{r\to\infty} f(r) = \infty$, such that*

$$A \cdot H_{mp^r}(\lambda, \mu) \equiv B \pmod{p^{f(r)}\mathbb{Z}} \tag{1.3}$$

for all sufficiently large r. Then $A = 1$, $B \in \{-2, -1, 0, 1, 2\}$, and (1.3) holds for all $r \geq 0$ with $f(r) = r + 1$.

(ii). *For every choice of λ, μ, p with p prime, there exist integers m, B such that the system of congruences* (1.2) *holds for all $r \geq 0$; furthermore we may choose $m = 1$ if $p = 2$; $m \leq 2$ if $p = 3$; and $m \leq (p^2-1)/2$ and dividing $p^2 - 1$ if $p \geq 5$.*

2. PRELIMINARIES AND EXISTENCE

For p a prime number, $\mathbb{Z}_p$, $\mathbb{Q}_p$, and $\mathbb{F}_{p^d}$ denote the ring of p-adic integers, the field of p-adic numbers, and the finite field of p^d elements, respectively. Let K be the splitting field of the characteristic polynomial $P(T) = 1 - \lambda T - \mu T^2$ over $\mathbb{Q}_p$, and write $P(T) = (1-\alpha T)(1-\beta T)$, where α, β are algebraic integers in K. We let $\mathfrak{O}_K$ denote the ring of algebraic integers of K, $\mathfrak{M}_K$ its unique maximal ideal, and $\bar{K} = \mathfrak{O}_K/\mathfrak{M}_K$ the residue-class field of K; for $x \in \mathfrak{O}_K$, $\bar{x}$ denotes its image in $\bar{K}$. There is an isomorphism $\bar{K} \cong \mathbb{F}_{p^d}$ where $d = 1$ or 2; we set $q = p^d$ and identify $\bar{K}$ with $\mathbb{F}_q$. If $x \in \mathfrak{O}_K$, the *Teichmüller representative* $\hat{x}$ of x is the unique element of $\mathfrak{O}_K$ satisfying $\hat{x} \equiv x \pmod{\mathfrak{M}_K}$ and $\hat{x}^q = \hat{x}$. It is easily seen that $\hat{x}$ is given by the p-adic limit $\hat{x} = \lim_{r\to\infty} x^{q^r}$. Our congruences are obtained from the well-known fact that $H_n(\lambda,\mu) = \alpha^n + \beta^n$ for all n and the congruences for powers of α, β given in ([4], Proposition 2).

Proof of Theorem 1. We first note that for all primes p and all positive integers m, r, we have the congruences

$$H_{mp^r}(\lambda,\mu) \equiv H_{mp^{r-1}}(\lambda,\mu) \pmod{p^r\mathbb{Z}}. \tag{2.1}$$

These were given in ([4], eq. (3.9)) in the case $\lambda = 1$, $\mu \neq -1$, but the argument given there is indeed valid as long as either λ or p is odd. When $p = 2$ and λ is even we give a similar proof, using ([4], Proposition 2 (iv)) to compute

$$\begin{aligned} H_{mp^r}(\lambda,\mu) &= \alpha^{mp^r} + \beta^{mp^r} \equiv 2\alpha^{mp^r} \equiv 2\alpha^{mp^{r-1}} \\ &\equiv \alpha^{mp^{r-1}} + \beta^{mp^{r-1}} = H_{mp^{r-1}}(\lambda,\mu) \pmod{2^r\mathfrak{O}_K}, \end{aligned} \tag{2.2}$$

but since both sides are integers, the congruence holds modulo $2^r\mathbb{Z}$. Therefore in all cases the sequence $\{H_{mp^r}(\lambda,\mu)\}_{r\geq 0}$ is a p-adically Cauchy sequence in $\mathbb{Z}_p$; since this sequence contains the subsequence $\{H_{mq^r}(\lambda,\mu)\}$, the limit as $r\to\infty$ must be $L = \lim_{r\to\infty}\alpha^{mq^r} + \beta^{mq^r} = \hat{\alpha}^m + \hat{\beta}^m$.

Equation (2.1) then shows that

$$H_{mp^r}(\lambda,\mu) \equiv L \pmod{p^{r+1}\mathbb{Z}_p}. \tag{2.3}$$

for all $r \geq 0$.

On the other hand, if (1.3) holds for large r, division by A yields

$$H_{mp^r}(\lambda,\mu) \equiv B/A \pmod{p^{f(r)-e}\mathbb{Z}_p} \tag{2.4}$$

for large r, where e is the p-adic ordinal of A. It follows that the sequence $\{H_{mp^r}(\lambda,\mu)\}$ converges p-adically to the rational number B/A. Since we already know this limit must be $L = \hat{\alpha}^m + \hat{\beta}^m$, and the Teichmüller representatives $\hat{\alpha}, \hat{\beta}$ are zero or roots of unity, we are led to consider the question,"When is a root of unity or a sum of two roots of unity a rational number?"

First there are the obvious real solutions, in which the sum of two elements of the set $\{-1,0,1\}$ gives an element of $\{-2,-1,0,1,2\}$. Now if ζ, ζ' are nonreal roots of unity then $\zeta+\zeta'$ is real if and only if $\zeta+\zeta' = 0$ or ζ' is the complex conjugate $\bar{\zeta}$ of ζ. For the second case, writing $\zeta = \cos\theta + i\sin\theta$ for some argument θ, we have $\zeta+\bar{\zeta} = 2\cos\theta$. If this is rational, say $\cos\theta = b/a$,then $\{\zeta,\bar{\zeta}\} = \{(b\pm\sqrt{b^2-a^2})/a\}$, whence ζ is an algebraic integer in $\mathbb{Q}(\sqrt{b^2-a^2})$ and therefore has degree 2 over $\mathbb{Q}$. But if ζ is a primitive m-th root of unity, then ζ has degree $\phi(m)$ over $\mathbb{Q}$ (where ϕ is Euler's totient), so $\phi(m) = 2$. This occurs if and only if $m = 3, 4$ or 6, and the corresponding sums $\zeta+\bar{\zeta}$ yield $-1, 0$, and 1, respectively. This proves that B/A lies in the set $\{-2,-1,0,1,2\}$, so the congruences $H_{mp^r}(\lambda,\mu) \equiv B/A$ in (2.3), (2.4) hold modulo $p^{r+1}\mathbb{Z}$ since both sides are integers. This completes the proof of (i).

For (ii), we note that $\bar{\alpha}, \bar{\beta}$ are either zero or have orders dividing $q-1$ in $\mathbb{F}_q^\times$, so we may choose $m > 0$ so that either $\bar{\alpha}^m, \bar{\beta}^m$ both lie in $\{-1,0,1\}$ or are two distinct elements of the same order $e = 3, 4$, or 6, as follows. If $p = 2$ then $q-1 = 1$ or 3, and if $\bar{\alpha}$ has order 3 then so does $\bar{\beta}$ and $\bar{\alpha} \neq \bar{\beta}$, so $m = 1$ always suffices; if $p = 3$ then $q-1 = 2$ or 8, and if $\bar{\alpha}$ has order $g \in \{4,8\}$ then $\bar{\beta}$

also has order g, and either they or their squares are distinct elements of order 4, so $m = 1$ suffices unless $g = 8$, in which case $m = 2$ works. For $p \geq 5$, $\bar{\alpha}, \bar{\beta}$ are either zero or have (possibly distinct) orders dividing $p - 1$; or else they have the same order g dividing $p^2 - 1$ but not $p - 1$. In the first case we may choose m dividing $(p-1)/2$ so that $\bar{\alpha}^m, \bar{\beta}^m \in \{-1, 0, 1\}$, and in the second case we choose m dividing g so that either $g/m = e \in \{3, 4, 6\}$ and $\bar{\alpha}^m, \bar{\beta}^m$ are *distinct* elements of order e if possible, or else that $g/m = e \in \{1, 2\}$. Since g divides $p^2 - 1$ we then have $m \leq (p^2 - 1)/2$. With this choice of m, $\hat{\alpha}^m, \hat{\beta}^m$ either both lie in $\{-1, 0, 1\}$ or are distinct primitive e-th roots of unity with $e = 3, 4$, or 6, so $L = \hat{\alpha}^m + \hat{\beta}^m$ lies in $\{-2, -1, 0, 1, 2\}$. Comparing with (2.3), we see that we have proven part (ii).

3. CHARACTERIZATIONS OF CONGRUENCES

In the course of proving Theorem 1 we have in fact established the following characterization of these congruences in terms of $\bar{\alpha}^m, \bar{\beta}^m$:

Theorem 2. *The congruences* (1.2) *hold for all* $r \geq 0$ *if and only if one of the following hold:*

(a). $B = 2$, *and* $\bar{\alpha}^m = \bar{\beta}^m = 1$ *in* $\mathbb{F}_q^\times$;

(b). $B = -2$, *and* $\bar{\alpha}^m = \bar{\beta}^m = -1$ *in* $\mathbb{F}_q^\times$ *with* $p > 2$;

(c). $B = 1$, *and either* $\{\bar{\alpha}^m, \bar{\beta}^m\} = \{0, 1\}$ *or* $\bar{\alpha}^m$, $\bar{\beta}^m$ *are distinct elements of order* 6 *in* $\mathbb{F}_q^\times$;

(d). $B = -1$, *and either* $\{\bar{\alpha}^m, \bar{\beta}^m\} = \{0, -1\}$ *with* $p > 2$, *or* $\bar{\alpha}^m$, $\bar{\beta}^m$ *are distinct elements of order* 3 *in* $\mathbb{F}_q^\times$;

(e). $B = 0$, *and either* $\bar{\alpha}^m = -\bar{\beta}^m$ *in* $\mathbb{F}_q^\times$ *with* $p > 2$, *or* $\bar{\alpha}^m = \bar{\beta}^m = 0$.

Remark. Since Teichmüller representatives satisfy $\hat{x}^q = \hat{x}$, they are either zero or roots of unity of order dividing $q - 1$. Thus for $p = 2$ the value -1 is not a Teichmüller representative since it has multiplicative order 2 which does not divide $q - 1$; this explains the clause "with $p > 2$" in (b) and (c). Furthermore, when $p = 2$, the Teichmüller representative of $-x$ is $\hat{x}$, not $-\hat{x}$, accounting for the clause "with $p > 2$" in (e). For $p = 2$ there are no elements of order 2, 4, or 6 in $\mathbb{F}_q^\times$ and for $p = 3$ there are no elements of order 3 or 6 in $\mathbb{F}_q^\times$.

Having given this description of the conditions for the congruences (1.2) in terms of $\bar{\alpha}^m, \bar{\beta}^m$, it is then natural to restate them in terms of λ, μ.

Corollary. (i). *For $p > 2$, the congruences (1.2) hold for all $r \geq 0$ with $B = 0$ if and only if they hold for $r = 1$ with $B = 0$; for $p = 2$ they hold for all $r \geq 0$ with $B = 0$ if and only if $\lambda \equiv \mu \equiv 0 \pmod{2\mathbb{Z}}$.*

(ii). *The congruences (1.2) hold for all $r \geq 0$ under the conditions on λ, μ, m, and B given in the following table. (Here $B = B_2$ (resp. B_3) if $p = 2$ (resp. 3) and there is an entry in the column B_2 (resp. B_3), and B is as in the first column otherwise). Furthermore for $B \neq 0$ and $(m, p^2 - 1) = 1$ this list is complete, i.e., the system of congruences (1.2) holds only under the conditions on λ, μ, and B given in the table.*

B	λ	μ	m	B_2	B_3
2	$1 \bmod p$	$-1 \bmod p$	$0 \bmod 6$		
2	$-1 \bmod p$	$-1 \bmod p$	$0 \bmod 3$		
2	$2 \bmod p$	$-1 \bmod p$	all		
2	$-2 \bmod p$	$-1 \bmod p$	even		
2	$0 \bmod p$	$-1 \bmod p$	$0 \bmod 4$		
2	$0 \bmod p$	$1 \bmod p$	even		
-2	$1 \bmod p$	$-1 \bmod p$	$3 \bmod 6$	2	
-2	$-2 \bmod p$	$-1 \bmod p$	odd	2	
-2	$0 \bmod p$	$-1 \bmod p$	$2 \bmod 4$	2	
1	$1 \bmod p$	$-1 \bmod p$	$\pm 1 \bmod 6$	-1	-2
1	$1 \bmod p$	$0 \bmod p$	all		
1	$-1 \bmod p$	$0 \bmod p$	even		
-1	$1 \bmod p$	$-1 \bmod p$	$\pm 2 \bmod 6$		2
-1	$-1 \bmod p$	$-1 \bmod p$	$\pm 1 \bmod 3$		2
-1	$-1 \bmod p$	$0 \bmod p$	odd	1	

Proof. For (i), we note that when p is odd, $B = \hat{\alpha}^m + \hat{\beta}^m = 0$ if and only if $\bar{\alpha}^m = -\bar{\beta}^m$, which is equivalent to $\alpha^m + \beta^m \equiv 0 \pmod{\mathfrak{M}_K}$, which is equivalent to $H_m(\lambda, \mu) \equiv 0 \pmod{p\mathbb{Z}}$. For $p = 2$ we have $B = 0$ if and only if $\bar{\alpha}^m = \bar{\beta}^m = 0$, which is equivalent to $\alpha^m \equiv \beta^m \equiv 0 \pmod{\mathfrak{M}_K}$, which is equivalent to $\lambda \equiv \mu \equiv 0 \pmod{2\mathbb{Z}}$.

For (ii), let us consider the case where $\lambda \equiv 1$ and $\mu \equiv -1 \pmod{p}$, which contains one of the cases treated in [1]. This means that $P(T) \equiv 1 - T + T^2 \pmod{p\mathbb{Z}[T]}$, so the reciprocal roots α, β of $P(T)$ satisfy

$$\alpha, \beta \equiv \frac{1 \pm \sqrt{-3}}{2} \pmod{\mathfrak{M}_K}. \tag{3.1}$$

If $p \geq 5$ then 6 divides $p^2 - 1$ and therefore the primitive sixth roots of unity $(1 \pm \sqrt{-3})/2$ are the Teichmüller representatives of their residue classes modulo $\mathfrak{M}_K$, so $\hat{\alpha}, \hat{\beta} = (1 \pm \sqrt{-3})/2$. It follows that $\hat{\alpha}^m, \hat{\beta}^m = (1 \pm \sqrt{-3})/2$ for any $m \equiv \pm 1 \pmod{6}$, and $B = \hat{\alpha}^m + \hat{\beta}^m = 1$ as in the tenth row of the table in this case. We similarly obtain $B = 1 + 1 = 2$ when $m \equiv 0 \bmod 6$, $B = -2$ when $m \equiv 3 \pmod{6}$, and $B = -1$ when $m \equiv \pm 2 \pmod{6}$, as in rows 1,7,and 13 of the table.

When $p = 3$ we have $\sqrt{-3} \equiv 0 \pmod{\mathfrak{M}_K}$, so (3.1) becomes $\alpha, \beta \equiv 1/2 \pmod{\mathfrak{M}_K}$. But $1/2 \equiv -1 \pmod{3\mathbb{Z}_3}$, so $\hat{\alpha}, \hat{\beta} = -1$ and therefore $B = (-1)^m + (-1)^m = 2(-1)^m$, giving the value B_3 in rows 10, 13 and the value B in rows 1, 7 of the table. This occurs because $\mathbb{F}_9^\times$ has no elements of order 6; the elements of multiplicative order 6 in K instead reduce to -1 in $\mathbb{F}_q$.

When $p = 2$, we note that α, β are negatives of the primitive cube roots of unity, and therefore

$$\alpha, \beta \equiv \frac{-1 \pm \sqrt{-3}}{2} \pmod{\mathfrak{M}_K}, \tag{3.2}$$

since $x \equiv -x \pmod{2\mathfrak{O}_K}$ for all $x \in \mathfrak{O}_K$. Since $\mathbb{F}_4^\times$ has elements of order 3 (but not of order 6) $\hat{\alpha}, \hat{\beta} = (-1 \pm \sqrt{-3})/2$ are the cube roots of unity. When m is not divisible by 3 we obtain $B = \hat{\alpha}^m + \hat{\beta}^m = -1$ as in rows 10, 13, whereas if m is a multiple of 3 we have $B = 1 + 1 = 2$ as in rows 1,7.

The other cases are handled similarly and the proofs are left to the reader. The special values B_2, B_3 occur because $\mathbb{F}_4^\times$ has no elements of order 2,4, or 6 and $\mathbb{F}_9^\times$ has no elements of order 3 or 6. For $p = 2$ all of the fourth roots of unity have Teichmüller representative 1; for $p = 3$ the primitive cube roots of unity have Teichmüller representative 1 and the primitive sixth roots of unity have Teichmüller representative -1.

To show that this list is complete when $B \neq 0$ and $(m, p^2 - 1) = 1$, we note that $1, 1 \pm T, 1 \pm T^2, 1 \pm T + T^2$, and $1 \pm 2T + T^2$ are the only integral polynomials with constant term 1 and degree at most 2 whose nonzero reciprocal roots in K have multiplicative order 1,2,3,4, or 6. Since $\mathbb{F}_q^\times$ is cyclic of order $p - 1$ or $p^2 - 1$, if $\bar{\alpha}^m, \bar{\beta}^m$ are zero or of order 1,2,3,4, or 6 then so are $\bar{\alpha}, \bar{\beta}$, whence $P(T)$ must be congruent modulo p to one of these polynomials. The cases $P(T) \equiv 1 \pm T^2 \pmod{p\mathbb{Z}[T]}$ with m odd and $P(T) \equiv 1 \pmod{p\mathbb{Z}[T]}$ are covered by (i) and the remaining cases occur in the table.

4. GENERALIZATIONS

We conclude by mentioning a few directions in which these results may be generalized. First, it will be noted that the theorems and proofs remain valid for $\lambda, \mu \in \mathbb{Z}_p$, not just in $\mathbb{Z}$, provided we replace "mod $p^a\mathbb{Z}$" with "mod $p^a\mathbb{Z}_p$" in the congruences (and in the conditions in the above table).

In general, since $L = \hat{\alpha}^m + \hat{\beta}^m$ is always an algebraic integer in $\mathbb{Q}(\zeta_{q-1})$ where ζ_{q-1} is a primitive $(q-1)$-st root of unity, we always have polynomial congruences for the sequence $\{H_{mp^r}(\lambda, \mu)\}$. Specifically, L is a root of some monic polynomial $T^k + a_{k-1}T^{k-1} + \cdots + a_1 T + a_0 \in \mathbb{Z}[T]$ of degree k (where $k = 1$ for $p = 2$ and $k \leq (q-1)/2$ for $p > 2$), so there are associated congruences of the form

$$H_{mp^r}(\lambda, \mu)^k + a_{k-1} H_{mp^r}(\lambda, \mu)^{k-1} + \cdots + a_1 H_{mp^r}(\lambda, \mu) + a_0 \equiv 0 \pmod{p^{r+1}\mathbb{Z}} \tag{4.1}$$

for every choice of λ, μ, m, and p. In this paper we have treated the case where such congruences exist with $k = 1$.

The Lucas sequences defined by the recursion (1.1) with initial conditions $H_0 = 0$, $H_1 = 1$ do not in general exhibit congruences of the form (1.2). From ([4], Corollary 1 (i)) we see that in this situation the sequence $\{H_{mq^r}\}_{r \geq 0}$ has a p-adic limit L but $\{H_{mp^r}\}_{r \geq 0}$ need not. The limit is

$L = (\hat{\alpha}^m - \hat{\beta}^m)/\sqrt{D}$ where $D = \lambda^2 + 4\mu$ is the discriminant of $P(T)$ (cf. [4], eq.(2.2)), and for this to be rational requires $\hat{\alpha}^m - \hat{\beta}^m = C\sqrt{D'}$ where $D = A^2 D'$ with $A, C, D' \in \mathbb{Z}$, since $\hat{\alpha}^m - \hat{\beta}^m$ must be an algebraic integer. Since the complex absolute value of $\hat{\alpha}^m - \hat{\beta}^m$ is at most 2, we need $C^2|D'| \leq 4$, so either $|D'| \leq 4$ or $C = 0$. These few possibilities may easily be determined but we see that, for example, congruences of this type with nonzero limit L cannot occur with squarefree discriminant D if $|D| > 3$ for this class of sequences.

These methods may be adapted, however, to prove congruences similar to (1.2) for the generalized Dickson polynomials g_n, which are generated by expansions of formal differentials

$$\frac{dP}{P} = -\sum_{n=0}^{\infty} g_n T^n \frac{dT}{T} \tag{4.2}$$

with characteristic polynomial $P(T) = 1 - a_1 T - a_2 T^2 - \cdots - a_m T^m$. (The present paper considers the case where $P(T)$ is quadratic). All such congruences yield identities in Galois rings, since e.g., a congruence $x \equiv y \pmod{p^r \mathbb{Z}}$ implies an equality $x = y$ in the Galois rings $GR(p^r, s)$.

Acknowledgement. The author thanks the referee for gently correcting a grievous error in the original manuscript.

REFERENCES

1. R. André-Jeannin. "On a Conjecture of Piero Filipponi", *The Fibonacci Quarterly*, **32.1** (1994), 11-14.
2. P. Filipponi. "A Note on a Class of Lucas Sequences", *The Fibonacci Quarterly*, **29.3** (1991), 256-263.
3. N. Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-functions*, Springer-Verlag, New York, 1977.
4. P. T. Young. "p-adic Congruences for Generalized Fibonacci Sequences", *The Fibonacci Quarterly*, **32.1** (1994), 2-10.

AMS Classification Numbers: 11B39, 11B50.