p-ADIC CONGRUENCES FOR GENERALIZED FIBONACCI SEQUENCES

Paul Thomas Young

Department of Mathematics, University of Charleston, Charleston, SC 29424

(*Submitted November 1991*)

1. STATEMENT OF RESULTS

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

$$\gamma_0 = 0, \ \gamma_1 = 1, \ \text{and} \ \gamma_{n+1} = \lambda\gamma_n + \mu\gamma_{n-1} \ \text{for} \ n > 0. \tag{1.1}$$

It is well known [9] that the polynomial $P(t) = 1 - \lambda t - \mu t^2$ has the property that

$$P(t)^{-1} = \sum_{n=1}^{\infty} \gamma_n t^{n-1} \tag{1.2}$$

is the ordinary formal power series generating function for the sequence $\{\gamma_{n+1}\}_{n\geq 0}$ (cf. [12]. Furthermore, it is easy to see [1] that when the discriminant $\Delta = \lambda^2 + 4\mu$ of $P(t)$ is nonnegative and $\lambda \neq 0$, the ratios γ_{n+1}/γ_n converge (in the usual archimedean metric on $\mathbb{R}$) to a reciprocal root α of $P(t)$. In this article we show that ratios of these γ_n also exhibit rapid convergence properties relating to $P(t)$ in the p-adic metrics on $\mathbb{Q}$. Precisely, we prove that for all primes p and all positive integers m the ratios $\gamma_{mp^r}/\gamma_{mp^{r-1}}$ converge p-adically in $\mathbb{Z}$; this is shown via congruences that extend those predicted by the theory of formal group laws (cf. [2], [7], [10]) or the theory of p-adic hypergeometric functions (cf. [13]). When p does not divide $\gamma_m\Delta$, these ratios converge to the quadratic character of Δ modulo p; otherwise, the limit is p or zero. Moreover, when $p > 3$ and p divides Δ, one obtains a supercongruence (cf. [2], [5], and eqs. (1.6), (3.8) below). These results are then used to give formal-group-law interpretations of some generalized Lucas sequences $\{\lambda_n\} = \{\gamma_{2n}/\gamma_n\}$, and of the sequence $\{T_n\} = \{F_{5n}/(5F_n)\}$ (where $\{F_n\}$ is the familiar Fibonacci sequence associated to $\lambda = \mu = 1$) which has been studied in [3]. The results are as follows.

Theorem 1: ***(i)*** If p is a prime not dividing $\gamma_m\Delta$, then for all $r \in \mathbb{Z}^+$ we have

$$\frac{\gamma_{mp^r}}{\gamma_{mp^{r-1}}} \equiv (\Delta \mid p) \pmod{p^r\mathbb{Z}}. \tag{1.3}$$

(ii) If p divides $\gamma_m\Delta$, then for all $r \in \mathbb{Z}^+$ such that $\gamma_{mp^{r-1}} \neq 0$ we have

$$\frac{\gamma_{mp^r}}{\gamma_{mp^{r-1}}} \equiv L \pmod{p^r\mathbb{Z}}, \tag{1.4}$$

where $L = 0$ or $L = p$ according to whether or not p divides μ.

(iii) The congruence (1.4) holds modulo $p^{r+1}\mathbb{Z}$ if $p > 2$ and p divides γ_m but not Δ; or if $(\Delta \mid p) = 0$ and either $p > 3$ or $p = 3$ and $r > 1$.

Corollary 1: ***(i)*** For all primes p and all $m, r \in \mathbb{Z}^+$ we have

$$\gamma_{mp^r} \equiv (\Delta | p)\gamma_{mp^{r-1}} \pmod{p^r\mathbb{Z}}. \tag{1.5}$$

(ii) If p divides γ_m but not Δ, then for all $r \in \mathbb{Z}^+$ we have

$$\gamma_{mp^r} \equiv L\gamma_{mp^{r-1}} \pmod{p^{2r}\mathbb{Z}}, \tag{1.6}$$

where $L = 0$ or $L = p$ according to whether or not p divides μ.

Theorem 2: Suppose $\lambda = 1$ and $\mu \neq -1$, and for $n > 0$ set $\lambda_n = \gamma_{2n} / \gamma_n$. Then the formal power series

$$\ell(t) = \sum_{n=1}^{\infty} \lambda_n \frac{t^n}{n} \tag{1.7}$$

is the logarithm of a one-dimensional formal group law over $\mathbb{Z}$ which is strictly isomorphic over $\mathbb{Z}$ to the formal multiplicative group law $\mathbb{G}_m(X, Y) = X + Y + XY$.

Theorem 3: Let $\{F_n\}$ denote the usual Fibonacci sequence, i.e., the solution to (1.1) in the case $\lambda = \mu = 1$, and for $n > 0$ set $T_n = F_{5n} / (5F_n)$. Then the formal power series

$$\tau(t) = \sum_{n=1}^{\infty} T_n \frac{t^n}{n} \tag{1.8}$$

is the logarithm of a one-dimensional formal group law over $\mathbb{Z}$ which is strictly isomorphic over $\mathbb{Z}$ to the formal multiplicative group law $\mathbb{G}_m(X, Y) = X + Y + XY$.

2. PRELIMINARY RESULTS

The congruences (1.5) of Corollary 1(i) are typical of those obtained from the theory of formal group laws; in fact (1.5) implies (via [10], Theorem A.8) that the formal differential $\omega = P(t)^{-1}\, dt$ is the canonical invariant differential on a formal group law over the ring $\mathbb{Z}_p$ of p-adic integers when $(\Delta | p) \neq 0$ (cf. eqs. (3.6), (3.7) below). Hazewinkel's book [7] is an excellent reference on formal group laws; the aspects of the theory most relevant to the present article are also summarized nicely in ([2], pp. 143-45; [5], §2.3; [10], Appendix). Our proof of Theorem 1, however, uses only the elementary theory of finite and p-adic fields; for an exposition of these topics, the reader is referred to [8].

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. We define $K = \mathbb{Q}_p(\sqrt{\Delta})$ if p does not divide Δ and $K = \mathbb{Q}_p(\sqrt{\Delta}, \sqrt{p})$ if p divides Δ. We let $\mathfrak{O}_K$ denote the ring of algebraic integers of K, $\mathfrak{M}_K$ its unique maximal ideal, and $\overline{K} = \mathfrak{O}_K / \mathfrak{M}_K$ the residue-class field of K; for $x \in \mathfrak{O}_K$, $\bar{x}$ denotes its image in $\overline{K}$. Let the positive integer d be defined so that $\overline{K} \cong \mathbb{F}_{p^d}$; then, 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 $\hat{x}^{p^d} = \hat{x}$. It is easily seen that $\hat{x}$ is given by the p-adic limit $\hat{x} = \lim_{r\to\infty} x^{p^{dr}}$.

If p is an odd prime and D is an integer, then $\sqrt{D} \in \mathbb{Z}_p$ if $(D|p)=1$ and $\sqrt{D} \notin \mathbb{Z}_p$ if $(D|p)=-1$; here $(\cdot|p)$ denotes the Legendre symbol. For ease of notation, we extend the definition of $(\Delta|p)$ to the case $p=2$ by

$$(\Delta|2) = \begin{cases} 1, & \text{if } \Delta \equiv 1 \pmod 8, \\ -1, & \text{if } \Delta \equiv 5 \pmod 8, \\ 0, & \text{if } \Delta \equiv 0 \pmod 4. \end{cases} \tag{2.1}$$

This is analogous to the Legendre symbol in that $\sqrt{\Delta} \in \mathbb{Z}_2$ if $(\Delta|2)=1$ and $\sqrt{\Delta} \notin \mathbb{Z}_2$ if $(\Delta|2)=-1$.

If $\Delta \neq 0$ then $P(t)=(1-\alpha t)(1-\beta t)$, where α, β are distinct elements of $\mathfrak{O}_K$. It is well known, and easily computed from (1.2), that in this case we have the Binet form

$$\gamma_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \tag{2.2}$$

for γ_n. It follows that, for all primes p and all positive integers m, r such that $\gamma_{mp^{r-1}} \neq 0$, we have

$$\frac{\gamma_{mp^r}}{\gamma_{mp^{r-1}}} = \frac{\alpha^{mp^r} - \beta^{mp^r}}{\alpha^{mp^{r-1}} - \beta^{mp^{r-1}}} = \Phi_p(\alpha^{mp^{r-1}}, \beta^{mp^{r-1}}), \tag{2.3}$$

where $\Phi_p(X,Y) = X^{p-1} + X^{p-2}Y + \cdots + XY^{p-2} + Y^{p-1}$ is the (two-variable) p^{th} cyclotomic polynomial.

Considering $P(t) \in \mathbb{R}[t]$, if $\Delta > 0$ then $\alpha, \beta \in \mathbb{R}$, and if $\lambda \neq 0$ then $\alpha \neq -\beta$; therefore, $\gamma_n \neq 0$ for all n if $\Delta > 0$ and $\lambda \neq 0$. However, when $\Delta < 0$ one can have $\gamma_n = 0$ in certain cases. We now show that this can only occur when $P(t)$ is equal to $1-t+t^2, 1-2t+2t^2$, $1-3t+3t^2$, or one of these polynomials with t replaced by kt for some integer k. We state Proposition 1 explicitly as follows.

Proposition 1: Suppose $P(t) = 1-\lambda t - \mu t^2 = (1-\alpha t)(1-\beta t)$ with $\lambda, \mu \in \mathbb{Z}$, and let $n \in \mathbb{Z}^+$. Then the following are equivalent:

(A) $\alpha^n = \beta^n$.

(B) One of the following holds:

- ***(i)*** $\Delta = 0$;
- ***(ii)*** n is even and $\lambda = 0$;
- ***(iii)*** n is divisible by 3, and $\lambda = k$, $\mu = -k^2$ for some $k \in \mathbb{Z}$;
- ***(iv)*** n is divisible by 4, and $\lambda = 2k$, $\mu = -2k^2$ for some $k \in \mathbb{Z}$;
- ***(v)*** n is divisible by 6, and $\lambda = 3k$, $\mu = -3k^2$ for some $k \in \mathbb{Z}$.

Proof: Suppose $\alpha^n = \beta^n$. If $n=1$, then $\alpha = \beta$, so $\Delta = (\alpha-\beta)^2 = 0$, as in (i). Now suppose $\alpha \neq \beta$; therefore, α, β, and Δ are all nonzero, so $\alpha^n = \beta^n$ implies $(\alpha/\beta)^n = 1$.

Choose m to be the minimal positive integer such that $(\alpha/\beta)^m = 1$; then $m > 1$ and $\alpha/\beta = \zeta_m$ is a primitive m^{th} root of unity. It follows that $\alpha^n = \beta^n$ if and only if n is a multiple of m. If $m = 2$, then $\alpha^2 = \beta^2$, so $\alpha = -\beta$, whence $\lambda = \alpha + \beta = 0$, as in (ii).

We now suppose $m > 2$; then ζ_m does not lie in $\mathbb{Q}$. The minimal polynomial of ζ_m over $\mathbb{Q}$ is the m^{th} cyclotomic polynomial $\Phi_m(X,1)$, which is irreducible of degree $\phi(m)$. [Here $\phi(m)$ denotes Euler's totient.] But $\zeta_m = \alpha/\beta$ lies in the quadratic field $\mathbb{Q}(\sqrt{\Delta})$, so the minimal polynomial of ζ_m has degree 2 over $\mathbb{Q}$. Thus, $\phi(m)=2$, which occurs precisely when $m = 3, 4,$ or 6.

For $m = 3$ we have $\Phi_3(X,1) = X^2+X+1$ and $\zeta_m = \alpha/\beta = (-1\pm\sqrt{-3})/2$, so $\arg(\alpha/\beta) = \pm 2\pi/3$. Since α and β are complex conjugates, $\arg(\alpha/\beta) = 2\arg(\alpha)$, whence $\arg(\alpha) = \pm\pi/3$ or $\pm 2\pi/3$. Therefore, $\alpha = k\cdot(1\pm\sqrt{-3})/2$ for some real scalar k, whence $P(t) = 1-kt+k^2t^2$. Since $P(t)\in\mathbb{Z}[t]$, we must have $k\in\mathbb{Z}$, precisely as in (iii). In this case, $\Delta = -3k^2$.

For $m = 4$, we have $\Phi_4(X,1) = X^2+1$ and $\zeta_m = \alpha/\beta = \pm\sqrt{-1}$, so $\arg(\alpha/\beta) = \pm\pi/2$. Thus, $\arg(\alpha) = \pm\pi/4$ or $\pm 3\pi/4$, so $\alpha = k\cdot(1\pm\sqrt{-1})$ for some real scalar k. Therefore, $P(t) = 1-2kt+2k^2t^2$, and since $P(t)\in\mathbb{Z}[t]$, we must have $k\in\mathbb{Z}$, precisely as in (iv). In this case, $\Delta = -4k^2$.

For $m = 6$, we have $\Phi_6(X,1) = X^2-X+1$ and $\zeta_m = \alpha/\beta = (1\pm\sqrt{-3})/2$, so $\arg(\alpha/\beta) = \pm\pi/3$. Thus, $\arg(\alpha) = \pm\pi/6$ or $\pm 5\pi/6$, or $\alpha = k\cdot(3\pm\sqrt{-3})/2$ for some real scalar k. Therefore, $P(t) = 1-3kt+3k^2t^2$, and since $P(t)\in\mathbb{Z}[t]$, we must have $k\in\mathbb{Z}$, precisely as in (v). In this case, $\Delta = -3k^2$.

We have shown that (A) implies (B). Using the above calculations, we find that (B) implies (A) by direct computation. This concludes the proof.

When $\gamma_m \neq 0$, it is also well known that $\varepsilon_m(n) = \lambda_{mn}/\lambda_m$ is an integer for all $n\in\mathbb{Z}^+$. In fact, it is easily seen from the Binet form (2.2) that $\varepsilon_m(n)$ satisfies the recursion (1.1) with λ and μ replaced by $\lambda_m = \alpha^m+\beta^m$ and $(-1)^{m-1}\mu^m = -\alpha^m\beta^m$, respectively, and the parameters $\lambda_m = \lambda\gamma_m + 2\mu\gamma_{m-1}$ and $(-1)^{m-1}\mu^m$ clearly lie in $\mathbb{Z}$. Our method will be to use (2.3) to deduce integral congruences for the integers $\gamma_{mp^r}/\gamma_{mp^{r-1}}$ from the following p-adic congruences for powers of α and β.

Proposition 2: Suppose $P(t) = 1-\lambda t-\mu t^2 = (1-\alpha t)(1-\beta t)$ with $\lambda,\mu\in\mathbb{Z}$.

- ***(i)*** If $(\Delta|p) = 1$, then $\alpha^{mp^r} \equiv \alpha^{mp^{r-1}} \pmod{p^r\mathbb{Z}_p}$;
- ***(ii)*** If $(\Delta|p) = -1$, then $\alpha^{mp^r} \equiv \beta^{mp^{r-1}} \pmod{p^r\mathfrak{O}_K}$;
- ***(iii)*** If $p>2$ and $(\Delta|p) = 0$, then $\alpha^{mp^r} \equiv \alpha^{mp^{r-1}} \equiv \beta^{mp^{r-1}} \equiv \beta^{mp^r} \pmod{p^{r-1/2}\mathfrak{O}_K}$;
- ***(iv)*** If $(\Delta|2) = 0$, then $\alpha^{m2^{r-1}} \equiv \beta^{m2^{r-1}} \pmod{2^r\mathfrak{O}_K}$ and $\alpha^{m2^{r-1}} \equiv \alpha^{m2^r} \pmod{2^{r-1}\mathfrak{O}_K}$.

Proof: If $x, y, p^s \in\mathfrak{O}_K$ and $x\equiv y \pmod{p^s\mathfrak{O}_K}$ write $x = y+z$ with $z\in p^s\mathfrak{O}_K$; then

$$x^p = y^p + \left(\sum_{k=1}^{p-1}\binom{p}{k}y^{p-k}z^k\right) + z^p \tag{2.4}$$

and hence $x^p \equiv y^p \pmod{p^{s+1}\mathfrak{O}_K}$ if $sp\geq s+1$. Thus, we need only prove these results in the case $r = 1$ and in addition that $a^{2m}\equiv a^{4m} \pmod{2\mathfrak{O}_K}$ when $(\Delta|2) = 0$; we may also assume $m = 1$ with no loss of generality.

If $(\Delta|p) = 1$, then $d = 1$, $K = \mathbb{Q}_p$, $\mathfrak{O}_K = \mathbb{Z}_p$, $\mathfrak{M}_K = p\mathbb{Z}_p$, and $\overline{K}\cong\mathbb{F}_p$. The statement $\alpha^p\equiv\alpha$ $\pmod{p\mathbb{Z}_p}$ is Fermat's little theorem, which proves (i) in the case $r = 1$.

If $(\Delta|p)=-1$, then $d=2$ and α,β are conjugates in the unramified extension K of $\mathbb{Q}_p$ (their minimal polynomial over $\mathbb{Q}_p$ is $t^2+\lambda\mu^{-1}t-\mu^{-1}$). We note that p does not divide μ, since if p divides μ then $\Delta\equiv\lambda^2\ (\mathrm{mod}\ 4p\mathbb{Z})$ and then $(\Delta|p)=1$. Therefore, α,β are units in $\mathfrak{O}_K$ (since $\alpha\beta=-\mu$), and $\overline{\alpha},\overline{\beta}$ are conjugates in $\overline{K}$ over $\mathbb{F}_p$ (their minimal polynomial being $t^2+\overline{\lambda}\overline{\mu}^{-1}t-\overline{\mu}^{-1}$). Since $\overline{K}\cong\mathbb{F}_{p^2}$ and $x\mapsto x^p$ is the nontrivial automorphism of $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$, we have $\overline{\alpha}^p=\overline{\beta}$ and $\overline{\beta}^p=\overline{\alpha}$; therefore, $\alpha^p\equiv\beta$ and $\beta^p\equiv\alpha$ modulo $\mathfrak{M}_K$. Since K is unramified, we have $\mathfrak{M}_K=p\mathfrak{O}_K$, yielding the $r=1$ case of (ii).

If $(\Delta|p)=0$, then q divides $\Delta=(\alpha-\beta)^2$, where $q=p$ if $p>2$ and $q=4$ if $p=2$. Therefore, $\alpha\equiv\beta\ (\mathrm{mod}\ q^{1/2}\mathfrak{O}_K)$, giving the middle congruence of (iii) and the first part of (iv) in the case $r=1$. As in (i) and (ii) above, we have $\alpha^p\equiv\alpha\text{ or }\beta\ (\mathrm{mod}\ \mathfrak{M}_K)$ according to whether $d=1$ or $d=2$, which completes (iii) for $r=1$, since $\mathfrak{M}_K=p^{1/2}\mathfrak{O}_K$. Finally, if $(\Delta|2)=0$, then 2 divides λ, and thus $\overline{\alpha},\overline{\beta}$ are roots of $t^2-\overline{\mu}^{-1}$; this shows that $\overline{K}\cong\mathbb{F}_2$ and so $\alpha,\beta\equiv 0\text{ or }1\ (\mathrm{mod}\ 2^{1/2}\mathfrak{O}_K)$. Writing $\alpha=y+z$ with $z\in 2^{1/2}\mathfrak{O}_K$ and $y=0$ or 1, we use (2.4) to check that $\alpha^2\in y+2\mathfrak{O}_K$ and $\alpha^4\in y+4\mathfrak{O}_K$, proving the $r=2$ case of the second statement of (iv).

Remarks: This proposition and its proof remain valid for λ,μ lying in $\mathbb{Z}_p$ (not just in $\mathbb{Z}$) provided one replaces the Legendre symbol with the Hilbert symbol. Furthermore, this proposition implies that, for each $m\in\mathbb{Z}^+$ and each prime p, the sequence $\{\alpha^{mp^{dr}}\}$ is a p-adically Cauchy sequence in $\mathfrak{O}_K$; the limit is the Teichmüller representative $\hat{\alpha}^m$.

3. DEMONSTRATION OF THEOREMS

Proof of Theorem 1: From Proposition 2(i), (ii), we have

$$\alpha^{mp^r}\equiv\begin{cases}\alpha^{mp^{r-1}}, & \text{if } (\Delta|p)=1,\\ \beta^{mp^{r-1}}, & \text{if } (\Delta|p)=-1,\end{cases}\quad(\mathrm{mod}\ p^r\mathfrak{O}_K),\tag{3.1}$$

and similarly for β^{mp^r}. Since $\Phi_p\in\mathbb{Z}[X,Y]$ and $\Phi_p(X,Y)=\Phi_p(Y,X)$, we have, in either case,

$$\frac{\gamma_{mp^r}}{\gamma_{mp^{r-1}}}=\Phi_p(\alpha^{mp^{r-1}},\beta^{mp^{r-1}})\equiv\Phi_p(\alpha^{mp^r},\beta^{mp^r})\equiv\cdots\equiv\Phi_p(\hat{\alpha}^m,\hat{\beta}^m)\ (\mathrm{mod}\ p^r\mathfrak{O}_K)\tag{3.2}$$

provided $\gamma_{mp^{r-1}}\neq 0$. Evaluating $\lim_{r\to\infty}\alpha^{mp^{dr}}$ using (3.1), we find that

$$\hat{\alpha}^{mp}=\begin{cases}\hat{\alpha}^m, & \text{if } (\Delta|p)=1,\\ \hat{\beta}^m, & \text{if } (\Delta|p)=-1.\end{cases}\tag{3.3}$$

If p does not divide $\gamma_m\Delta=(\alpha-\beta)(\alpha^m-\beta^m)$, then $\hat{\alpha}^m\neq\hat{\beta}^m$; therefore, $\gamma_{mp^{r-1}}\neq 0$ for all r. Thus, we have

$$\Phi_p(\hat{\alpha}^m,\hat{\beta}^m)=\frac{\hat{\alpha}^{mp}-\hat{\beta}^{mp}}{\hat{\alpha}^m-\hat{\beta}^m}=(\Delta|p).\tag{3.4}$$

Together with (3.2) this shows that $\gamma_{mp^r}/\gamma_{mp^{r-1}} \equiv (\Delta|p) \pmod{p^r\mathfrak{O}_K}$; since both sides of this congruence are integers, the congruence must hold modulo $p^r\mathbb{Z}$, completing the proof of (i).

As in (3.2), one can see from Proposition 2 that, provided $\gamma_{mp^{r-1}}$ is always nonzero, one has $\Phi_p(\hat{\alpha}^m, \hat{\beta}^m)$ as the p-adic limit of $\gamma_{mp^r}/\gamma_{mp^{r-1}}$, and thus determine the value L as stated in part (ii) of the theorem. One may discover the stronger congruences of (iii) [which will be useful in the proofs of Corollary 1(ii) and Theorem 3], however, by making a simple algebraic manipulation.

Suppose that p divides $\gamma_m\Delta$; then write $x_r = \alpha^{mp^{r-1}}$, $y_r = \beta^{mp^{r-1}}$, $z_r = x_r - y_r$, and

$$\frac{\gamma_{mp^r}}{\gamma_{mp^{r-1}}} = \frac{x_r^p - y_r^p}{x_r - y_r} = \frac{(y_r + z_r)^p - y_r^p}{z_r} = py_r^{p-1} + \left(\sum_{k=2}^{p-1}\binom{p}{k}y_r^{p-k}z_r^{k-1}\right) + z_r^{p-1}. \tag{3.5}$$

If p divides $\gamma_m = (\alpha^m - \beta^m)/(\alpha - \beta)$ but not $\Delta = (\alpha - \beta)^2$, then $\alpha^m \equiv \beta^m \pmod{p\mathfrak{O}_K}$; therefore, $\hat{\alpha}^m = \hat{\beta}^m$. Since $\{\overline{\alpha}^p, \overline{\beta}^p\} = \{\overline{\alpha}, \overline{\beta}\}$ and $\overline{\alpha}^m = \overline{\beta}^m$, we have $\overline{\alpha}^m = \overline{\beta}^m \in \mathbb{F}_p$; thus, $\hat{\alpha}^m = \hat{\beta}^m \in \mathbb{Z}_p$. Note that $\hat{\alpha}, \hat{\beta} \neq 0$ since p does not divide Δ; hence, p does not divide $\mu = -\alpha\beta$, and by Fermat's little theorem, $\hat{\beta}^{m(p-1)} = 1$. From Proposition 2(i), (ii), we have $\alpha^{mp^{r-1}} \equiv \hat{\alpha}^m = \hat{\beta}^m \equiv \beta^{mp^{r-1}} \pmod{p^r\mathfrak{O}_K}$. Therefore, the term py_r^{p-1} in (3.5) is congruent to p modulo $p^{r+1}\mathfrak{O}_K$. The final term z_r^{p-1} is zero modulo $p^{r(p-1)}\mathfrak{O}_K$, which shows that $\gamma_{mp^r}/\gamma_{mp^{r-1}} \equiv p \pmod{p^r\mathfrak{O}_K}$; since both sides are integers, the congruence holds modulo $p^r\mathbb{Z}$, as asserted in (ii). In fact, since $r(p-1) \geq r+1$ for $p > 2$ and $r > 0$, we see that the congruence (1.3) holds modulo $p^{r-1}\mathbb{Z}$ when $p > 2$ and p divides γ_m but not Δ.

The case $(\Delta|p) = 0$, $\Delta \neq 0$ is similar; using Proposition 2(iii) we find that for $p > 2$ the term py_r^{p-1} in (3.5) is congruent to $p\hat{\beta}^{m(p-1)}$ modulo $p^{r+1/2}\mathfrak{O}_K$, all terms within the summation in (3.5) are zero modulo $p^{r+1/2}\mathfrak{O}_K$, and the final term z_r^{p-1} is zero modulo $p^{(r-1/2)(p-1)}\mathfrak{O}_K$. Thus, for $p > 2$, we have $\gamma_{mp^r}/\gamma_{mp^{r-1}} \equiv L \pmod{p^r\mathfrak{O}_K}$ and, therefore, modulo $p^r\mathbb{Z}$. In addition, since $(r-1/2)(p-1) \geq r + 1/2$ for $p > 3$ or for $p = 3$ and $r > 1$, in these cases the congruence (1.4) holds modulo $p^{r+1}\mathbb{Z}$, since it holds modulo $p^{r+1/2}\mathfrak{O}_K$ while both sides lie in $\mathbb{Z}$. If $(\Delta|2) = 0$, we find from Proposition 2(iv) that $2\alpha^{m2^{r-1}} \equiv L \pmod{2^r\mathfrak{O}_K}$ and $z_r \equiv 0 \pmod{2^r\mathfrak{O}_K}$, giving the result in that case.

Finally, if $\Delta = 0$, then $P(t) = (1-\alpha t)^2$ for some $\alpha \in \mathbb{Z}$, and a quick computation from (1.2) yields $\gamma_n = n\alpha^{n-1}$. If $\lambda \neq 0$, then $\alpha \neq 0$; therefore, we have $\gamma_{mp^r}/\gamma_{mp^{r-1}} = p\alpha^{mp^{r-1}(p-1)} \in \mathbb{Z}$. As in Proposition 2(i), if p does not divide α this lies in $p + p^{r+1}\mathbb{Z}$, whereas if $\alpha \in p\mathbb{Z}$, it is clearly congruent to zero modulo $p^{r+1}\mathbb{Z}$.

Proof of Corollary 1: We first treat the case where $\Delta > 0$ and $\lambda \neq 0$ so that $\gamma_n \neq 0$ for all n. If p does not divide $\gamma_m\Delta$, part (i) follows directly from (1.4) upon multiplication by $\gamma_{mp^{r-1}}$. From Theorem 1(ii), we find by induction on r that $\gamma_{mp^r} \equiv 0 \pmod{p^{r+1}\mathbb{Z}}$ if p divides γ_m, and $\gamma_{mp^r} \equiv 0 \pmod{p^r\mathbb{Z}}$ if p divides Δ. It then follows that both sides of (1.5) are zero modulo $p^r\mathbb{Z}$ if p divides $\gamma_m\Delta$.

For (ii), we recall from Theorem 1(iii) that the congruence (1.4) holds modulo $p^{r+1}\mathbb{Z}$ when $p>3$ and p divides Δ. In this case or in the case where p divides γ_m, we obtain (ii) upon multiplication of (1.4) by $\gamma_{mp^{r-1}}$.

To extend these results to arbitrary Δ and λ, we observe that if $\lambda' = \lambda + p^N$ and γ'_n is defined by $\gamma'_0 = 0, \gamma'_1 = 1$, and $\gamma'_{n+1} = \lambda'\gamma'_n + \mu\gamma'_{n-1}$, then $\gamma'_n \equiv \gamma_n \pmod{p^N\mathbb{Z}}$ for all n. It is clear that we may choose N large enough so that $N \ge 2r$, $\Delta' = (\lambda')^2 + 4\mu > 0$, and $\lambda' \ne 0$. Since $\Delta' \equiv \Delta \pmod{p\mathbb{Z}}$, the results for any Δ, λ follow from the results for Δ', λ'.

Remarks: One can easily determine from [4] with the aid of §5.8 in [7] that $\omega = P(t)^{-1}\,dt$ is the canonical invariant differential on the formal group law $F(X,Y)$ over $\mathbb{Z}$ given by the rational function

$$F(X,Y) = (X+Y-\lambda XY)/(1+\mu XY) \tag{3.6}$$

(equivalently, $\Sigma_{n=1}^{\infty}\gamma_n T^n/n$ is the logarithm of this formal group law). From this, it follows ([2]; [10], Theorem A.8) that there exist congruences of the type

$$\gamma_{mp^r} \equiv H\gamma_{mp^{r-1}} \pmod{p^r\mathbb{Z}_p} \tag{3.7}$$

for some $H \in \mathbb{Z}_p$, when p does not divide γ_p [which is equivalent, via Corollary 1(i), to the condition $(\Delta|p) \ne 0$]. What is surprising about Corollary 1 is that the congruences obtained also hold, and are in fact stronger, in the cases not predicted by the theory of formal group laws [i.e., when $(\Delta|p) = 0$]. Other congruences of the type

$$c_{mp^r} \equiv Hc_{mp^{r-1}} \pmod{p^{ar}\mathbb{Z}_p} \tag{3.8}$$

with $a \ge 2$ (called "supercongruences") have also been observed involving binomial coefficients [6] and the Apéry numbers [2], and have been conjectured in [11].

Proof of Theorem 2: The statement that the formal power series (1.7) is the logarithm of a formal group law over $\mathbb{Z}$ which is strictly isomorphic over $\mathbb{Z}$ to $\mathbb{G}_m$ is equivalent to requiring that $\lambda_n \in \mathbb{Z}, \lambda_1 = 1$, and for all primes p and all $m, r \in \mathbb{Z}^+$ the congruences

$$\lambda_{mp^r} \equiv \lambda_{mp^{r-1}} \pmod{p^r\mathbb{Z}} \tag{3.9}$$

(cf. [2], pp. 143-45; [10], Theorem A.9). Assuming $\lambda = 1$ and $\mu \ne -1$, Proposition 1 tells us that γ_n is never zero, so $\lambda_n \in \mathbb{Z}$ for $n>0$ and, from (2.3), we have $\lambda_n = \alpha^n + \beta^n$. We have $\lambda = \lambda_1 = 1$ and $\Delta = \lambda^2 + 4\mu$ is odd, so it follows from Proposition 2(i), (ii), (iii), that the congruences (3.9) hold modulo $p^{r-1/2}\mathfrak{O}_K$, but both sides are integers, so the theorem follows.

Proof of Theorem 3: From [3] we know that $T_n \in \mathbb{Z}$ for all n, and it is clear that $T_1 = 1$. Therefore, as in Theorem 2, we must show that for all primes p and all $m, r \in \mathbb{Z}^+$, we have

$$T_{mp^r} \equiv T_{mp^{r-1}} \pmod{p^r\mathbb{Z}} \tag{3.10}$$

From the definition of T_n, one has

$$T_n = \frac{1}{5}\Phi_5(\alpha^n, \beta^n), \tag{3.11}$$

where α, β are the reciprocal roots of the polynomial $P(t) = 1 - t - t^2$ associated to $\lambda = \mu = 1$. Since $\Delta = 5$, for all primes $p \neq 5$ these congruences follow directly from Proposition 2(i), (ii), as in (3.2). To complete the proof, we take advantage of the fact that

$$\frac{F_{m5^r}}{F_{m5^{r-1}}} \equiv 5 \,(\bmod\, 5^{r+1}\mathbb{Z}), \tag{3.12}$$

which is a consequence of Theorem 1(iii). Dividing by 5, we obtain

$$T_{m5^{r-1}} = \frac{F_{m5^r}}{5F_{m5^{r-1}}} \equiv 1 \,(\bmod\, 5^r\mathbb{Z}), \tag{3.13}$$

which proves the congruence (3.10) in the case $p = 5$, completing the proof.

Remark: The result (3.13) is not best possible; in fact, the congruence $T_{5^r} \equiv 1 \pmod{5^{2r}\mathbb{Z}}$ has been shown in ([3], Lemma 2).

4. CONCLUDING REMARKS

In [3] it is noted that for $k \in \mathbb{Z}^+$ the sequences $\{T(k,n)\}_{n>0}$ given by $T(k,n) = F_{kn}/(F_kF_n)$ are always integral in the three special cases $k = 1$ [$T(1,n) = 1$ for all n], $k = 2$ [$T(2,n) = L_n$, the n^{th} Lucas number], and $k = 5$ [$T(5,n) = T_n$]. Our Theorem 2 and Theorem 3 explain that all three of these sequences occur as the expansion coefficients for the logarithms of formal group laws over $\mathbb{Z}$ which are strictly isomorphic over $\mathbb{Z}$ to the same formal group law $\mathbb{G}_m$.

For $p \neq 2$ one may also approach these p-adic properties of the sequence $\{\gamma_n\}$ via its combinatorial form

$$\gamma_{n+1} = \sum_{k=0}^{[n/2]} \binom{n-k}{k} \lambda^{n-2k}\mu^k \tag{4.1}$$

[9], which may be expressed in terms of hypergeometric functions as

$$\gamma_{n+1} = \lambda^n \, {}_2F_1\left(\begin{matrix} -n/2,\ (1-n)/2 \\ -n \end{matrix}; -4\mu/\lambda^2\right) \tag{4.2}$$

We sketch the method here: Taking $n+1 = mp^r$ and letting $r \to \infty$, the parameters $-n/2$, $(1-n)/2$, and $-n$ converge p-adically to 1/2, 1, and 1, respectively. Using a suitable modification of the argument in ([13], Theorem 4.1) one can show that when p does not divide γ_p, the p-adic limit of $\gamma_{p^r}/\gamma_{p^{r-1}}$ is given by

$$\lim_{r\to\infty} \frac{\gamma_{p^r}}{\gamma_{p^{r-1}}} = {}_2\mathfrak{F}_1\left(\begin{matrix} \frac{1}{2}, 1 \\ 1 \end{matrix}; \widehat{(-4\mu/\lambda^2)}\right), \tag{4.3}$$

where (as in the notation of [13]) the symbol ${}_2\mathfrak{F}_1(x)$ denotes the p-adic "analytic continuation" of ${}_2F_1(x)/{}_2F_1(x^p)$. Since ${}_2F_1(1/2,1;1;x) = {}_1F_0(1/2;;x) = (1-x)^{-1/2}$, the same value for the p-adic limit in (4.3) is also obtained from $\lim_{r\to\infty}(c_{p^r}/c_{p^{r-1}})$, where

But clearly $\lim_{r\to\infty}(c_{p^r}/c_{p^{r-1}}) = \lim_{r\to\infty}\Delta^{p^{r-1}(p-1)/2} = \hat{\Delta}^{(p-1)/2}$, which is seen to be precisely $(\Delta|p)$ from Euler's criterion

$$(\Delta|p) \equiv \Delta^{(p-1)/2} \pmod{p\mathbb{Z}} \tag{4.5}$$

and the fact that $\widehat{(\pm 1)} = \pm 1$. The point is that the sequences $\{\gamma_{n+1}\}$ and $\{\Delta^{n/2}\}$ should have the same p-adic congruence behavior because they arise from hypergeometric functions that are p-adically proximate (when $n+1 = mp^r$) So, if one is willing to appeal to the p-adic analytic properties of the combinatorial form (4.1), one may obtain a fair explanation for the occurrence of $(\Delta|p)$ in Theorem 1(i) when $(\Delta|p) \neq 0$. But again, Theorem 1(ii) shows that the p-adic limit in (4.3) even exists when $(\Delta|p) = 0$ [which is equivalent to p dividing γ_p, by Corollary 1(i)], a fact that is not predicted by the theory of p-adic hypergeometric functions (cf. [13], Theorem 2.3).

ACKNOWLEDGMENTS

The author thanks James E. Carter for an inspiring discussion, and the referee for useful comments and suggestions.

REFERENCES

1. R. André-Jeannin. "A Note on the Irrationality of Certain Lucas Infinite Series." *The Fibonacci Quarterly* **29.2** (1991):132-36.
2. F. Beukers. "Some Congruences for the Apéry Numbers." *J. Number Theory* **21** (1985): 141-55.
3. M. Bucci, A. Di Porto, & P. Filipponi. "A Note on the Sequence $\{F_{5n}/(5F_n)\}$." Preprint.
4. R. Coleman & F. McGuinness. "Rational Formal Group Laws." *Pacific J. Math.* **147** (1991):25-27.
5. M. Coster. *Supercongruences.* Leiden, 1988.
6. M. Coster. "Generalization of a Congruence of Gauss." *J. Number Theory* **29** (1988):300-310.
7. M. Hazewinkel. *Formal Groups and Applications.* New York: Academic Press, 1978.
8. N. Koblitz. *p-Adic Numbers, p-Adic Analysis, and Zeta-Functions.* New York: Springer-Verlag, 1977.
9. P. McCarthy & R. Sivaramakrishnan. "Generalized Fibonacci Sequences via Arithmetical Functions." *The Fibonacci Quarterly* **28.4** (1900):363-70.
10. J. Stienstra & F. Beukers. "On the Picard-Fuchs Equation and the Formal Brauer Group of Certain Elliptic *K*3-Surfaces." *Math. Annalen* **271** (1985):269-304.
11. L. van Hamme. "Proof of a Conjecture of Beukers on Apéry Numbers." *Proceedings of the Conference on p-Adic Analysis, Hengelhoef* (1986):189-95.
12. H. Wilf. *Generatingfunctionology.* Boston-San Diego-New York: Academic Press, 1990.
13. P. T. Young. "Apéry Numbers, Jacobi Sums, and Special Values of Generalized p-Adic Hypergeometric Functions." *J. Number Theory* **41** (1992):231-55.

AMS Classification Numbers: 11B39, 11A15

❖❖❖