SOME DIVISIBILITY PROPERTIES OF GENERALIZED FIBONACCI SEQUENCES

PAUL S. BRUCKMAN
4213 Lancelot Drive, Concord, CA 94521

1. INTRODUCTION

Let c be any square-free integer, p any odd prime such that $(c/p) = -1$, and n any positive integer. The quantity $\sqrt{c}$, which would ordinarily be defined (mod p^n) as one of the two solutions of the congruence: $x^2 \equiv c$ (mod p^n), does not exist. Nevertheless, we may deal with objects of the form $a + b\sqrt{c}$ (mod p^n), where a and b are integers, in much the same way that we deal with complex numbers, the essential difference being that $\sqrt{-1}$'s role is assumed by $\sqrt{c}$. Since we are dealing with congruences (mod p^n), we may without loss of generality restrict a and b to a particular residue class (mod p^n), the most convenient for our purpose being the minimal residue class (mod p^n). Accordingly, we define the sets $R_n(p)$ and $R_n(p,c)$ as follows:

$$(1) \qquad R_n(p) = \left\{a : a \text{ an integer, } |a| \leq \tfrac{1}{2}(p^n - 1)\right\};$$

$$(2) \qquad R_n(p,c) = \left\{z : z = a + b\sqrt{c}, \text{ where } a,b \in R_n(p)\right\}.$$

In the sequel, congruences will be understood to be (mod p^n), unless otherwise indicated, and we will omit the modulus designation, for brevity, provided no confusion is likely to arise. The symbol "$\equiv$" denotes congruence and should not be confused with the identity relation.

We also define the set $R(p,c)$ as follows:

$$(3) \qquad R(p,c) = \left\{z : z = a + b\sqrt{c}, \text{ where } a \text{ and } b \text{ are rational numbers whose numerators and denominators are prime to } p\right\}.$$

The set $R_n(p,c)$ satisfies all of the usual laws of algebra, and its elements may be manipulated in much the same way as complex numbers, provided we identify the "real" and "imaginary" parts of $z = a + b\sqrt{c}$, namely a and b, respectively.

If $z = (a + b\sqrt{c}) \in R_n(p,c)$ and $(ab,p) = 1$, then z has a multiplicative inverse in $R_n(p,c)$, denoted by z^{-1}, given by

$$(4) \qquad z^{-1} \equiv (a^2 - b^2c)^{-1}(a - b\sqrt{c}),$$

where $(a^2 - b^2c)^{-1}$ is the inverse of $(a^2 - b^2c)$, all operations reduced (mod p^n), in such a manner that $(a^2 - b^2c)$, its inverse, and z^{-1} are in $R_n(p,c)$. The condition $(ab,p) = 1$ is both necessary and sufficient to ensure that z^{-1} exists. Two elements $z_k = a_k + b_k\sqrt{c}$, $k = 1, 2$, of $R(p,c)$ are said to be *congruent (mod p^n)* (or more simply *congruent*) iff $a_1 \equiv a_2$ and $b_1 \equiv b_2$. They are said to be *conjugate* iff $a_1 \equiv a_2$ and $b_1 \equiv -b_2$. Hence, every element of $R_n(p,c)$ has a unique conjugate in $R_n(p,c)$, and every element of $R_n(p)$ is (trivially) self-conjugate.

It is not difficult to show that $R_n(p,c)$, which is the set in which we are really interested, is a commutative ring with identity; moreover, $R_1(p,c)$ is a field.

Next, we recall some basic results of "ordinary" number theory. For all $z \in R_n(p)$, such that $(z,p) = 1$,

(5) $$z^{\frac{1}{2}\phi(p^n)} \equiv \left(\frac{z}{p}\right),$$

(6) $$z^{\phi(p^n)} \equiv 1$$ [where $\phi(p^n) = (p - 1)p^{n-1}$ is the Euler (totient) function].

Note that (5) implies (6), which is a generalization of Fermat's Theorem. A more general formulation of (6) is the following:

(7) $$z^{p^n} \equiv z^{p^{n-1}}, \text{ for all } z \in R_n(p).$$

The following theorem generalizes the last result even further.

Theorem 1: For all $z \in R_n(p,c)$,

(8) $$z^{p^n} \equiv (\bar{z})^{p^{n-1}}.$$

Proof: We will first prove (8) for the case $n = 1$, then proceed by induction on n. Suppose $z = (a + b\sqrt{c}) \in R_n(p,c)$. Then, by the binomial theorem,

$$z^p = (a + b\sqrt{c})^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k}(b\sqrt{c})^k \equiv a^p + (b\sqrt{c})^p \pmod{p},$$

since $p \mid \binom{p}{k}$ for $k = 1, 2, \ldots, p - 1$. But $a^p \equiv a$ and $b^p \equiv b \pmod{p}$ [by (7), with $n = 1$]. Since $\left(\frac{c}{p}\right) = -1$, thus $z^p \equiv \bar{z} \pmod{p}$, which is the result of (8) for the case $n = 1$, $[(\sqrt{c})^p = c^{\frac{1}{2}(p-1)}\sqrt{c} \equiv \left(\frac{c}{p}\right)\sqrt{c} = -\sqrt{c}$, by (5)].

Let S denote the set of natural numbers n such that (8) holds for all $z \in R_n(p,c)$. We have just shown that $1 \in S$. Suppose $m \in S$. Then $z^{p^m} = \bar{z}^{p^{m-1}} + wp^m$, for some $w \in R_1(p,c)$. Therefore,

$$(z^{p^m})^p = z^{p^{m+1}} = (\bar{z}^{p^{m-1}} + wp^m)^p \equiv \bar{z}^{p^m} + p\bar{z}^{(p-1)p^{m-1}}wp^m \equiv \bar{z}^{p^m} \pmod{p^{m+1}}.$$

Thus, $m \in S \Rightarrow (m + 1) \in S$. The result now follows by induction.

Given any $z = (a + b\sqrt{c}) \in R(p,c)$, there exists a unique

$$z^* = (a^* + b^*\sqrt{c}) \in R_n(p,c),$$

such that $a \equiv a^*$, $b \equiv b^*$, i.e., $z \equiv z^*$. Moreover, $1/z = (a - b\sqrt{c})/(a^2 - b^2c)$ and $(z^*)^{-1}$ both exist and $1/z \equiv (z^*)^{-1}$. These properties may be deduced from the preceding discussion. Therefore, when no confusion is likely to arise, we will omit the "starred" notation in the sequel, and treat elements of $R(p,c)$ as elements of $R_n(p,c)$ interchangeably, though the reader should bear the technical distinction in mind.

2. APPLICATIONS TO GENERALIZED FIBONACCI SEQUENCES

Suppose $u = (a + b\sqrt{c}) \in R(p,c)$, $v = \bar{u} = a - b\sqrt{c}$, where $2a$ is an integer, $(a^2 - b^2c) = \pm 1$. Define the sequences $\{\varphi_k\}$ and $\{\lambda_k\}$ as follows:

(9) $$\varphi_k = \frac{u^k - v^k}{u - v},$$

(10) $$\lambda_k = u^k + v^k,\ k = 0, 1, 2, \ldots .$$

As is commonly known, the φ's and λ's are integers and satisfy the same recursion:

(11) $$\gamma_{k+2} = 2a\gamma_{k+1} + (b^2c - a^2)\gamma_k.$$

Note that $b \not\equiv 0 \pmod{p}$, which implies $(u - v)^{-1} = (2b\sqrt{c})^{-1} \equiv w \in R_n(p,c)$. Hence, we may treat $\{\varphi_k\}$ and $\{\lambda_k\}$ as sequences in $R_n(p)$. By application of Theorem 1, we may deduce certain divisibility properties of these sequences (mod p^n). To illustrate, we prove the following

Theorem 2: Given u and v as defined above, if $m = m(p,n) = (p + 1)p^{n-1}$, then

(12) $$\varphi_m \equiv 0, \text{ and}$$

(13) $$\lambda_m \equiv 2(a^2 - b^2c).$$

Proof: By Theorem 1,

$$u^{p^n} \equiv v^{p^{n-1}},\quad v^{p^n} \equiv u^{p^{n-1}}.$$

Hence,

$$u^{p^n}u^{p^{n-1}} \equiv v^{p^n}v^{p^{n-1}} \equiv (uv)^{p^n},$$

i.e.,

$$u^m \equiv v^m \equiv (a^2 - b^2c)^{p^n} \equiv (a^2 - b^2c).$$

Note that $(u - v)^{-1}$ exists. Hence, applying the definitions in (9) and (10), the result of Theorem 2 now follows.

The preceding theorem eloquently illustrates the power of the method of "complex residues." By dealing with certain nebulous objects of the form $a + b\sqrt{c} \pmod{p^n}$, which have no "real" meaning in the modular arithmetic, we have deduced some purely number-theoretic results about generalized Fibonacci and Lucas sequences. The analogy with bona fide complex numbers and their applications should now be more evident.

A somewhat stronger result than (13) is actually true, but the method of complex residues does not appear to be of help in such fortification. We will first state the strengthened result, then state and prove a number of lemmas, returning finally to the proof.

Theorem 3: Let u, v, and m be defined as in Theorem 2. Then

(14) $$\lambda_m \equiv 2(a^2 - b^2c) \pmod{p^{2n}}.$$

Lemma 1: Let λ_k be as given in (10). Then

(15) $$\sum_{i=0}^{[\frac{1}{2}n]} (-1)^i \frac{n}{n-i}\binom{n-i}{i}\lambda_{2s}^{n-2i} = \lambda_{2ns} \quad (s = 0, 1, 2, \ldots;\ n = 1, 2, 3, \ldots).$$

Proof: We may prove the result by generating functions. Alternatively, the following, essentially, is formula (1.64) in [1]:

(16) $$\sum_{i=0}^{\left[\frac{1}{2}n\right]} \frac{\binom{n-i}{i}}{n-i}\left(\frac{1}{4}z\right)^i = \frac{1}{n2^{n-1}}\left(\frac{x^n + y^n}{x + y}\right), \text{ where } x = 1 + \sqrt{z+1},\ y = 1 - \sqrt{z+1}.$$

In (16), let $z = -4/\lambda_{2s}^2$ (note $\lambda_{2s} \neq 0\ \forall\ s$). Then

$$\sqrt{z+1} = \frac{\sqrt{\lambda_{2s}^2 - 4}}{\lambda_{2s}} = \frac{u^{2s} - v^{2s}}{\lambda_{2s}} = \frac{(u - v)\varphi_{2s}}{\lambda_{2s}}.$$

Hence,

$$x = 2u^{2s}/\lambda_{2s}, \quad y = 2v^{2s}/\lambda_{2s}, \quad x + y = 2.$$

Substituting in (16), we obtain:

$$\sum_{i=0}^{\left[\frac{1}{2}n\right]} \frac{\binom{n-i}{i}}{n-i}(-1)^i \lambda_{2s}^{-2i} = \frac{1}{n2^{n-1}}\left(\frac{2^n(u^{2ns} + v^{2ns})}{\lambda_{2s}^n \cdot 2}\right).$$

This simplifies to (15), proving the lemma.

Lemma 2:

$$\sum_{i=0}^{\left[\frac{1}{2}n\right]} (-1)^i \frac{n}{n-i}\binom{n-i}{i}2^{n-2i} = 2 \qquad (n = 1, 2, 3, \ldots).$$

Proof: Let $s = 0$ in Lemma 1.

Lemma 3:

$$\sum_{i=0}^{\left[\frac{1}{2}n\right]} (-1)^i \binom{n-i}{i}2^{n-2i} = n + 1 \qquad (n = 0, 1, 2, \ldots).$$

Proof: This is formula (1.72) in [1].

Lemma 4:

(17) $$\sum_{i=0}^{\left[\frac{1}{2}n\right]} (-1)^i (n - 2i)\frac{n}{n-i}\binom{n-i}{i}2^{n-1-2i} = n^2 \qquad (n = 1, 2, 3, \ldots).$$

Proof: The left member of (17) is equal to

$$\sum_{i=0}^{\left[\frac{1}{2}n\right]} (-1)^i (2n - 2i - n)\frac{n}{n-i}\binom{n-i}{i}2^{n-1-2i}$$

$$= n\sum_{i=0}^{\left[\frac{1}{2}n\right]} (-1)^i \binom{n-i}{i}2^{n-2i} - \frac{1}{2}n\sum_{i=0}^{\left[\frac{1}{2}n\right]} (-1)^i \frac{n}{n-i}\binom{n-i}{i}2^{n-2i}$$

$$= n(n+1) - \frac{1}{2}n \cdot 2 = n^2 \qquad \text{(using Lemmas 2 and 3).}$$

Proof of Theorem 3: From Theorem 1, with $n = 1$, $u^p \equiv v$, $v^p \equiv u \pmod{p}$. Hence, since $\bar{u} = v$, there exists $w \in R_1(p,c)$, such that

(18) $$u^p \equiv v + pw, \quad v^p \equiv u + p\bar{w} \pmod{p^2}.$$

Multiplying these last two congruences, we have:

$$(uv)^p \equiv uv + p(uw + \overline{uw}) \pmod{p^2}.$$

However, $uv = a^2 - b^2c = \pm 1$, so $(uv)^p = uv$. Hence, it follows that

(19) $$uw + \overline{uw} \equiv 0 \pmod{p}.$$

If, in (18), we multiply throughout by u and v, respectively, we obtain:

$$u^{p+1} \equiv uv + puw, \quad v^{p+1} \equiv uv + p\overline{uw} \pmod{p^2}.$$

Now adding these last two congruences and using (19), we obtain the result

(20) $$\lambda_{p+1} \equiv 2(a^2 - b^2c) \pmod{p^2}.$$

This is (13) for the case $n = 1$. Let T be the set of natural numbers n for which (13) holds; we have shown that $1 \in T$. Suppose $r \in T$, and let

$$m_1 = (p+1)p^{r-1}.$$

By Lemma 1, since m_1 is even,

$$\lambda_{pm_1} = \sum_{i=0}^{\frac{1}{2}(p-1)} (-1)^i \frac{p}{p-i}\binom{p-i}{i}\lambda_{m_1}^{p-2i}.$$

But, by the inductive hypothesis, $\lambda_{m_1} = 2uv + Kp^{2r}$, for some integer K. Hence,

$$\begin{aligned}
\lambda_{pm_1} &= \sum_{i=0}^{\frac{1}{2}(p-1)} (-1)^i \frac{p}{p-i}\binom{p-i}{i}(2uv + Kp^{2r})^{p-2i} \\
&= \sum_{i=0}^{\frac{1}{2}(p-1)} (-1)^i \frac{p}{p-i}\binom{p-i}{i}\sum_{j=0}^{p-2i}\binom{p-2i}{j}(2uv)^{p-2i-j}(Kp^{2r})^j \\
&= \sum_{j=0}^{p}(Kp^{2r})^j \sum_{i=0}^{\left[\frac{1}{2}(p-j)\right]} (-1)^i \frac{p}{p-i}\binom{p-i}{i}\binom{p-2i}{j}(2uv)^{p-2i-j} \\
&\equiv \sum_{i=0}^{\frac{1}{2}(p-1)} (-1)^i \frac{p}{p-i}\binom{p-i}{i}(2uv)^{p-2i} \\
&\quad + Kp^{2r}\sum_{i=0}^{\frac{1}{2}(p-1)} (-1)^i \left(\frac{p}{p-i}\right)(p-2i)\binom{p-i}{i}(2uv)^{p-2i-1} \pmod{p^{2r+2}} \\
&\equiv uv\sum_{i=0}^{\frac{1}{2}(p-1)} (-1)^i \frac{p}{p-i}\binom{p-i}{i}2^{p-2i} \\
&\quad + Kp^{2r}\sum_{i=0}^{\frac{1}{2}(p-1)} (-1)^i \frac{p}{p-i}\binom{p-i}{i}(p-2i)2^{p-2i-1} \pmod{p^{2r+2}} \\
&\equiv 2uv + Kp^{2r+2} \pmod{p^{2r+2}} \equiv 2uv \pmod{p^{2r+2}}
\end{aligned}$$

(using Lemmas 2 and 4). Hence, $r \in T \Rightarrow (r+1) \in T$. The result of the theorem now follows by induction.

Corollary 1 (of Theorems 2 and 3):

Let p be any odd prime such that $\left(\frac{5}{p}\right) = -1$, n be any natural number, and $m = m(p,n) = (p+1)p^{n-1}$. Then

(21) $$F_m \equiv 0 \pmod{p^n}, \text{ and}$$

(22) $$L_m \equiv -2 \pmod{p^{2n}}.$$

Proof: Let $a = b = \frac{1}{2}$, $c = 5$, and apply (12) and (14) and the definitions of Fibonacci and Lucas sequences.

3. THE CASE $\left(\frac{c}{p}\right) = 1$

We will now deal with the case where $\left(\frac{c}{p}\right) = 1$, starting our discussion anew. We soon find that this case is much simpler than the first, since now $\sqrt{c}$ is an element of $R_n(p)$, in the modular sense, and thus has a "real" meaning. In fact, if all the definitions of the preceding discussion are retained with the exception that now $\left(\frac{c}{p}\right) = 1$, we see that objects $(a + b\sqrt{c})$ of $R(p,c)$ are actually congruent (mod p^n) to objects of $R_n(p)$, and that we do not need to concern ourselves with $R_n(p,c)$ at all. In other words, the theory of "complex residues" is irrelevant in this simpler case. With this idea in mind, we may "rethink" the results of the previous section. Thus, Theorem 1 is replaced by (7), for the case $\left(\frac{c}{p}\right) = 1$. The counterpart of Theorem 2 is the following, for this case.

Theorem 4: Let the sequences $\{\varphi_k\}$ and $\{\lambda_k\}$ be given by (9) and (10), and let $M = (p-1)p^{n-1} = \phi(p^n)$. Then

(23) $$\varphi_M \equiv 0, \text{ and}$$

(24) $$\lambda_M \equiv 2.$$

Proof: By (6), $u^M \equiv v^M \equiv 1$, which implies: $u^M - v^M \equiv 0$, $u^M + v^M \equiv 2$. Since $(u - v)^{-1} = (2b\sqrt{c})^{-1}$ exists, we may apply the definitions in (9) and (10), thereby proving the result.

The counterpart of Theorem 3 is the following fortification of (24):

Theorem 5:

(25) $$\lambda_M \equiv 2 \pmod{p^{2n}}.$$

Proof: BY (7), with $n = 1$, $u^p \equiv u$, $v^p \equiv v \pmod{p}$. Thus, there exist x and y in $R_1(p)$ such that

(26) $$u^p \equiv u + px, \quad v^p \equiv v + py \pmod{p^2}.$$

Multiplying these two congruences, we obtain: $(uv)^p \equiv uv + p(uy + vx) \pmod{p^2}$. But $uv = \pm 1$, so $(uv)^p = uv$. Hence, we have

(27) $uy + vx \equiv 0 \pmod{p}$.

Returning to (26), if we multiply throughout by v and u, respectively, we obtain: $u^{p-1}(uv) \equiv uv + p(vx)$, $v^{p-1}(uv) \equiv uv + p(uy) \pmod{p^2}$. Now, adding these last two congruences and using (27), we have: $uv(u^{p-1} + v^{p-1}) \equiv 2uv \pmod{p^2}$, which implies (25) for the case $n = 1$.

The remainder of the proof of Theorem 5 is nearly identical to that of Theorem 3, except that in the latter, we replace m_1 by $M_1 = (p - 1)p^{r-1}$.

4. SUMMARY AND CONCLUSION

We may combine Theorems 2 thru 5 thus far derived into the following main theorem. For the sake of completeness and clarity, we will incorporate the necessary definitions in the hypothesis of the theorem.

Theorem 6: Let c be any square-free integer, p any odd prime such that $c \not\equiv 0 \pmod{p}$, and n any positive integer. Let a and b be any rational numbers such that neither their numerators nor their denominators are divisible by p, $2a$ is an integer, and $(a^2 - b^2c) = \pm 1$. Let

$$u = a + b\sqrt{c},\ v = a - b\sqrt{c},\ \varphi_n = (u^n - v^n)/(u - v),\ \lambda_n = u^n + v^n.$$

Finally, let

$$m = m(n,p) = \left\{p - \left(\frac{c}{p}\right)\right\}p^{n-1}.$$

Then

(28) $\varphi_m \equiv 0 \pmod{p^n}$, and

(29) $\lambda_m \equiv 1 + uv + (1 - uv)\left(\frac{c}{p}\right) \pmod{p^{2n}}$.

Corollary 2: Let $\{F_k\}$ and $\{L_k\}$ be the Fibonacci and Lucas sequences. Let p be any odd prime $\neq 5$, and $m = \left\{p - \left(\frac{5}{p}\right)\right\}p^{n-1}$, $n = 1, 2, 3, \ldots$. Then

(30) $F_m \equiv 0 \pmod{p^n}$, and

(31) $L_m \equiv 2\left(\frac{5}{p}\right) \pmod{p^{2n}}$.

Proof: Let $a = b = \frac{1}{2}$, $c = 5$ in Theorem 6.

Corollary 3: Let $\{P_k\}$ and $\{Q_k\}$ be the Pell and "Lucas-Pell" sequences ($a = b = 1$, $c = 2$ in Theorem 6). Let p be any odd prime, and $m = \left\{p - \left(\frac{2}{p}\right)\right\}p^{n-1}$, $n = 1, 2, 3, \ldots$. Then

(32) $P_m \equiv 0 \pmod{p^n}$, and

(33) $Q_m \equiv 2\left(\frac{2}{p}\right) \pmod{p^{2n}}$.

Theorem 6 is the main result of this paper. However, it should be clear to the reader that the basic result of Theorem 1 may be used to obtain other types of congruences, where the indices of the generalized Fibonacci or Lucas sequences are other than the "m" of Theorem 6. The corresponding results, however, do not appear to be quite as elegant as that of Theorem 6. Nevertheless, some information may be gathered about the periodicity (mod p^n) of the sequences in question. For example, using the methods of this paper, we may deduce that, if $P(N)$ denotes the period (mod N) of the Fibonacci and Lucas sequence (the periods for the two sequences *are* the same, except when $5|N$, cf. [2]), and if p is any odd prime $\neq 5$, then

(34) $$p(p^n) \text{ divides } \frac{1}{2}\left(3p + 1 - (p + 3)\left(\frac{5}{p}\right)\right)p^{n-1},\quad n = 1, 2, 3, \ldots .$$

We will leave the proof of this result to the reader.

REFERENCES

1. H. W. Gould, *Combinatorial Identities* (Morgantown, W.Va.: The Morgantown Printing and Binding Co., 1972).
2. Dov Jarden, *Recurring Sequences* (Jerusalem: Riveon Lematematika, 1973), p. 103.
3. G. H. Hardy & E. M. Wright, *An Introduction to the Theory of Numbers* (4th ed., reprinted; Oxford: The Clarendon Press, 1962), pp. 221-223.

A NOTE ON A PELL-TYPE SEQUENCE

WILLIAM J. O'DONNELL
George Washington High School, Denver, CO

The Pell sequence is defined by the recursive relation

$$P_1 = 1,\ P_2 = 2, \text{ and } P_{n+2} = 2P_{n+1} + P_n, \text{ for } n \geq 1.$$

The first few terms of the sequence are 1, 2, 5, 12, 29, 70, 169, 408, ... It is well known that the nth term of the Pell sequence can be written

$$P_n = \frac{1}{\sqrt{8}}\left[\left(\frac{2+\sqrt{8}}{2}\right)^n - \left(\frac{2-\sqrt{8}}{2}\right)^n\right].$$

It is also easily proven that $\lim_{n\to\infty} \frac{P_n}{P_{n+1}} = \frac{-2+\sqrt{8}}{2}$.

For the sequence $\{V_n\}$ defined by the recursive formula

$$V_1 = 1,\ V_2 = 2, \text{ and } V_{n+2} = kV_{n+1} + V_n, \text{ for } k \geq 1,$$

we know that

$$\lim_{n\to\infty} \frac{V_n}{V_{n+1}} = \frac{-k + \sqrt{k^2+4}}{2}.$$

If we let $k = 1$, the sequence $\{V_n\}$ becomes the Fibonacci sequence and the limit of the ratio of consecutive terms is $\frac{-1+\sqrt{5}}{2} = .618$, which is the "golden ratio." For $k = 2$ the ratio becomes .4142, which is the limit of the ratio of consecutive terms of the Pell sequence.

Both of the previous sequences were developed by adding two terms of a sequence or multiples of two terms to generate the next term. We now consider the ratio of consecutive terms of the sequence $\{G_n\}$ defined by the recursive formula

$$G_1 = a_1,\ G_2 = a_2,\ \ldots,\ G_n = a_n, \text{ and}$$

and