◆◇◆◇◆

ON SOME DIVISIBILITY PROPERTIES OF FIBONACCI AND RELATED NUMBERS

GERHARD ROSENBERGER
Universität Dortmund, Federal Republic of Germany

(Submitted April 1982)

1. Let x be an arbitrary natural number. We define, recursively, the following two sequences of rational integers.

$$S_{-1}(x) = -1,\ S_0(x) = 0,\ S_n(x) = xS_{n-1}(x) - S_{n-2}(x),\ n \geqslant 1. \tag{1}$$

$$R_{-1}(x) = 1,\ R_0(x) = 0,\ R_n(x) = xR_{n-1}(x) + R_{n-2}(x),\ n \geqslant 1 \tag{2}$$

If $x = 1$ and $n \geqslant 0$, then $R_n(x)$ is the nth Fibonacci number. By mathematical induction, we immediately obtain

$$R_{2n}(x) = xS_n(x^2 + 2) \tag{3}$$

and

$$R_{2n-1}(x) = S_n(x^2 + 2) - S_{n-1}(x^2 + 2),\ \text{where } n \in \mathbf{N} \cup \{0\}. \tag{4}$$

The purpose of this note is to look at some divisibility properties of the natural numbers $R_n(x)$ that are of great interest to some subgroup problems for the general linear group $GL(2, \mathbf{Z})$.

Of the many papers dealing with divisibility properties for Fibonacci numbers, perhaps the most useful are those of Bicknell [1], Bicknell & Hoggatt [2], Hairullin [4], Halton [5], Hoggatt [6], Somer [9], and the papers which are cited in these. Numerical results are given in [3]. Some of our results are known or are related to known results but are important for our purposes. As far as I know, the other results presented here are new or are at least generalizations of known results.

2. Let p be a prime number. Let $n(p, x)$ be the subscript of the first positive number $R_n(x)$, $n \geqslant 1$, divisible by p.

If p divides x, then

$$n(p, x) = 2.$$

If $p = 2$ and x is odd, then

$$n(p, x) = 3.$$

Henceforth, let p always be an odd prime number that does not divide x. Then it is known that $n(p, x)$ divides $p - \varepsilon$, $\varepsilon = 0, 1$, or -1, where

$$\varepsilon = \left(\frac{x^2 + 4}{p}\right)$$

is Legendre's symbol (cf., for instance, [7]).

We want to prove some more intrinsic results about $n(p, x)$. For this we make use of the next five identities; the proof of these identities is computational.

$$R_{n+3}(x) = (x^2 + 2)R_{n+1}(x) - R_{n-1}(x); \tag{5}$$

$$R_{kn}(x) = S_k(R_{n+1}(x) + R_{n-1}(x)) \cdot R_n(x) \text{ if } n \text{ is even}, \tag{6a}$$

$$R_{kn}(x) = R_k(R_{n+1}(x) + R_{n-1}(x)) \cdot R_n(x) \text{ if } n \text{ is odd}; \tag{6b}$$

$$R_{n+1}(x)R_{n-1}(x) - R_n^2(x) = (-1)^n; \tag{7}$$

$$R_{n+2}^2(x) - R_{n+4}(x)R_n(x) = (-1)^n x^2; \tag{8}$$

$$R_{2n-1}(x) = R_n^2(x) + R_{n-1}^2(x), \tag{9a}$$

$$xR_{2n}(x) = R_{n+1}^2(x) - R_{n-1}^2(x); \tag{9b}$$

where $n \in \mathbf{N} \cup \{0\}$.

3. The case $n(p, x)$ odd.

Let $n(p, x) = 2m - 1$, $m \in \mathbf{N}$; it is $m \geqslant 2$.

Proposition 1

a. $R_{2m+1}(x) \equiv -R_{2m-3}(x) \pmod{p}$.

b. $R_{2m-3}^2(x) \equiv -x^2 \pmod{p}$.

c. $R_{2m-2}^2(x) \equiv -1 \pmod{p}$.

d. $R_{2m-1-k}(x) \equiv (-1)^{k+1}R_k(x)R_{2m-2}(x) \pmod{p}$ for all integers k with $0 \leqslant k \leqslant 2m - 1$.

Proof: Statements (a), (b), and (c) follow directly from (3), (5), (7), and (8).

We now prove statement (d) by mathematical induction. Statement (d) is true for $k = 0$ and $k = 1$ because $R_{2m-1}(x) \equiv 0 \pmod{p}$ and $R_1(x) = 1$. Now we suppose that statement (d) is true for all integers ℓ with $0 \leqslant \ell \leqslant k$, where $1 \leqslant k < 2m - 1$.

For $1 \leqslant k < 2m - 1$ and k even, we obtain

$$\begin{aligned} R_{2m-1-(k+1)}(x) &\equiv -xR_{2m-1-k}(x) + R_{2m-1-(k-1)}(x) \\ &\equiv (xR_k(x) + R_{k-1}(x)) \cdot R_{2m-2}(x) \\ &\equiv (-1)^{k+2}R_{k+1}(x)R_{2m-2}(x) \pmod{p}. \end{aligned}$$

For $1 \leqslant k < 2m - 1$ and k odd, we obtain

$$\begin{aligned} R_{2m-1-(k+1)}(x) &\equiv (-xR_k(x) - R_{k-1}(x)) \cdot R_{2m-2}(x) \\ &\equiv (-1)^{k+2}R_{k+1}(x)R_{2m-2}(x) \pmod{p}. \end{aligned}$$

Q.E.D.

Corollary 1

$p \equiv 1 \pmod 4$.

Proof: Proposition 1 gives that -1 is a quadratic residue mod p. That means

$$1 = \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2},$$

and, therefore, $p \equiv 1 \pmod 4$. Q.E.D.

Proposition 2

If $p \equiv 1 \pmod 4$, then there is a natural number z such that

$$z^2 + 1 \equiv 0 \pmod p$$

and

$$(xz + 1)R_{m-1}^2(x) \equiv z^{2m} \pmod p.$$

Proof: From (9) we get

$$R_m^2(x) \equiv -R_{m-1}^2(x) \pmod p.$$

Then there is a natural number z such that

$$z^2 + 1 \equiv 0 \pmod p$$

and

$$R_m(x) \equiv zR_{m-1}(x) \pmod p.$$

Therefore,

$$R_{m+1}(x) \equiv xR_m(x) + R_{m-1}(x) \equiv (xz + 1)R_{m-1}(x) \pmod p$$

and

$$z^{2m} \equiv (-1)^m \equiv R_{m+1}(x)R_{m-1}(x) - R_m^2(x) \equiv (xz + 2)R_{m-1}^2(x) \pmod p$$

by (7). Q.E.D.

The following corollary is an immediate consequence.

Corollary 2

If $p \equiv 1 \pmod p$, then there is a natural number z such that

$$z^2 + 1 \equiv 0 \pmod p$$

and $xz + 2$ is a quadratic residue mod p.

Remark concerning Proposition 2: If $p = 4q + 1$, $q \geqslant 1$, and g is a primitive root mod p, then $z \equiv \pm g^q \pmod p$. But unfortunately, no direct method is known for calculating primitive roots in general without a great deal of computation, especially for large p.

Proposition 3

Let $n \geqslant 1$ be a natural number such that p divides $R_{2n-1}(x)$. Then

$$R_{2(k+1)-1}(x) \cdot S_{n-k}(x^2+2) \equiv R_{2k-1}(x) \cdot S_{n-(k+1)}(x^2+2) \pmod{p},$$

for all integers k with $0 \leqslant k \leqslant n$.

Proof by mathematical induction: The statement is true for $k = 0$, since

$$S_n(x^2+2) \equiv S_{n-1}(x^2+2) \pmod{p} \quad [\text{by } (4)].$$

Now suppose the statement is true for an integer k with $0 \leqslant k < n$. Then we obtain

$$R_{2k-1}(x) \cdot S_{n-(k+1)}(x^2+2) \equiv R_{2k+1}(x) \cdot S_{n-k}(x^2+2)$$
$$\equiv \left((x^2+2)S_{n-(k+1)}(x^2+2) - S_{n-(k+2)}(x^2+2)\right) \cdot R_{2k+1}(x) \pmod{p}.$$

This gives

$$\begin{aligned} R_{2(k+1)-1}(x) &\cdot S_{n-(k+2)}(x^2+2) \\ &\equiv \left((x^2+2)R_{2k+1}(x) - R_{2k-1}(x)\right) \cdot S_{n-(k+1)}(x^2+2) \\ &\equiv R_{2(k+1)-1}(x) \cdot S_{n-(k+1)}(x^2+2) \pmod{p} \quad [\text{by } (5)]. \text{ Q.E.D.} \end{aligned}$$

Corollary 3

a. $0 \not\equiv R_{2(m-1)-1}(x) \cdot S_{m-k}(x^2+2) \equiv R_{2k-1}(x) \pmod{p}$ for all integers k with $0 \leqslant k \leqslant m-1$.

b. $R_{2(k+\ell)-1}(x) \cdot S_{m-k}(x^2+2) \equiv R_{2k-1}(x) \cdot S_{m-(k+\ell)}(x^2+2) \pmod{p}$ for all integers k and ℓ with $0 \leqslant k$, $0 \leqslant \ell$, and $0 \leqslant k+\ell \leqslant m$.

Proof: Statement (b) is obviously true for $k = m$ (if $k = m$ then $\ell = 0$); statements (a) and (b) are also obviously true for $k = m - 1$. Now, letting $0 \leqslant k \leqslant m-2$, we obtain (from Proposition 1)

$$\begin{aligned} R_{2k-1}(x) &\cdot R_{2k+1}(x) \cdot S_{m-(k+2)}(x^2+2) \\ &\equiv R_{2k-1}(x) \cdot R_{2k+3}(x) \cdot S_{m-(k+1)}(x^2+2) \\ &\equiv R_{2k+3}(x) \cdot R_{2k+1}(x) \cdot S_{m-k}(x^2+2) \pmod{p}, \end{aligned}$$

which gives

$$R_{2(k+2)-1}(x) \cdot S_{m-k}(x^2+2) \equiv R_{2k-1}(x) \cdot S_{m-(k+2)}(x^2+2) \pmod{p}$$

because $R_{2k+1}(x) \not\equiv 0 \pmod{p}$.

Now, by mathematical induction, we obtain

$$R_{2(k+\ell)-1}(x) \cdot S_{m-k}(x^2+2) \equiv R_{2k-1}(x) \cdot S_{m-(k+\ell)}(x^2+2) \pmod{p}$$

for all integers k and ℓ with $0 \leqslant k$, $0 \leqslant \ell$, and $0 \leqslant k+\ell \leqslant m$ (this statement is trivial for $\ell = 0$ and just Proposition 3 for $\ell = 1$). Now statement (b) is proved; statement (a) follows for $k + \ell = m - 1$. Q.E.D.

4. The case $n(p, x)$ even. Let $n(p, x) = 2m$, $m \in \mathbf{N}$; it is $m \geqslant 2$ because p does not divide x. Moreover, $S_m(x^2 + 2) \equiv 0 \pmod p$ by (3).

Proposition 4

$$(x^2 + 4)R_{m-1}^2(x) \equiv (-1)^{m+1}x^2 \pmod p.$$

Proof: From (6), we get

$$-R_{m-1}(x) \equiv R_{m+1}(x) \equiv xR_m(x) + R_{m-1}(x) \pmod p$$

and

$$xR_m(x) \equiv -2R_{m-1}(x) \pmod p$$

because $n(p, x)$ is minimal. Therefore,

$$(-1)^m x^2 \equiv x^2(R_{m+1}(x)R_{m-1}(x) - R_m^2(x)) \equiv -(x^2 + 4)R_{m-1}^2(x) \pmod p$$

by (7). Q.E.D.

Corollary 4

If $p \equiv 1 \pmod 4$, then $x^2 + 4$ is a quadratic residue mod p.

Proof: If $p \equiv 1 \pmod 4$, then $\left(\frac{-1}{p}\right) = 1$ and the statement follows immediately from Proposition 4. Q.E.D.

If we ask for prime numbers p' with $p' \equiv 1 \pmod 4$ and $\left(\frac{x^2 + 4}{p'}\right) = -1$, we obtain the following.

Corollary 5 (Special Cases)

a. If $x = 1$, then $p \not\equiv q \pmod{20}$, where $q = 13$ or 17.

b. If $x = 2$ or 4, then $p \not\equiv 5 \pmod 8$.

c. If $x = 3$, then $p \not\equiv q \pmod{52}$, where $q = 5, 21, 33, 37, 41$, or 45.

d. If $x = 5$, then $p \not\equiv q \pmod{116}$, where $q = 17, 21, 37, 41, 61, 69, 73, 77, 85, 89, 97, 101, 105$, or 113.

Analogous to Proposition 1, Proposition 3, and Corollary 3, we obtain the following results.

Proposition 5

a. $R_{2m+2}(x) \equiv -R_{2m-2}(x) \pmod p$.

b. $R_{2m-2}^2(x) \equiv x^2 S_{m-1}(x^2 + 2) \equiv x^2 \pmod p$.

c. $R_{2m-1}^2(x) \equiv 1 \pmod p$.

d. $R_{2m-k}(x) \equiv (-1)^{k+1}R_k(x)R_{2m-1}(x) \pmod p$
for all integers k with $0 \leqslant k \leqslant 2m$.

Proposition 6

Let $n \geqslant 1$ be a natural number such that p divides $R_{2n}(x)$. Then

$$R_{2k}(x) \cdot S_{n-(k+1)}(x^2+2) \equiv R_{2(k+1)}(x) \cdot S_{n-k}(x^2+2) \pmod{p}$$

for all integers k with $0 \leqslant k \leqslant n$.

Corollary 6

a. $0 \not\equiv R_{2(m-1)}(x) \cdot S_{m-k}(x^2+2) \equiv R_{2k}(x) \pmod{p}$
for all integers k with $0 \leqslant k \leqslant m-1$.

b. $R_{2(k+\ell)}(x) \cdot S_{m-k}(x^2+2) \equiv R_{2k}(x) \cdot S_{m-(k+\ell)}(x^2+2) \pmod{p}$
for all integers k and ℓ with $0 \leqslant k$, $0 \leqslant \ell$, and $0 \leqslant k+\ell \leqslant m$.

5. Final Remark. I wish to thank the referee for two relevant references that were not included in the original version of the paper. He also noted that some results of this paper are special cases of results of Somer [9] for the sequence

$$T_0(x, y) = 0,\ T_1(x, y) = 1,\ T_n(x, y) = xT_{n-1}(x, y) + yT_{n-2}(x, y),\ n \geqslant 2,$$

where x and y are arbitrary rational integers. Proposition 1(c) is a special case of Somer's Theorem 8(i); Proposition 2 is a special case of his Lemma 3(i) and the proof of his Lemma 4 when one takes into account the hypothesis that $(-1)/(p) = 1$; Corollary 4 is a special case of Somer's Lemma 3(ii) and (iii); finally, Proposition 5(c) is a special case of his Theorem 8(i).

But, on the other side, some results of Somer's paper follow directly from known results about the numbers $S_n(x)$ and $R_n(x)$. For, let x and y now be arbitrary complex numbers with $y \neq 0$. Let $S_n(x)$, $R_n(x)$, and $T_n(x, y)$ be analogously defined as above. Then

$$T_n(x, y) = (\sqrt{-y})^{n-1} S_n\left(\frac{x}{\sqrt{-y}}\right) = (\sqrt{y})^{n-1} R_n\left(\frac{x}{\sqrt{y}}\right),\quad n \geqslant 0,$$

where $\sqrt{y}$ and $\sqrt{-y}$ are suitably determined (see, for instance, [7]).

REFERENCES

1. M. Bicknell. "A Primer for the Fibonacci Numbers: Part VII, An Introduction to Fibonacci Polynomials and Their Divisibility Properties." *The Fibonacci Quarterly* 8, No. 4 (1970):407-20.
2. M. Bicknell & V. E. Hoggatt, Jr., eds. *Fibonacci's Problem Book.* San Jose, Calif.: The Fibonacci Association, 1974.
3. Brother U. Alfred Brousseau. *Tables of Fibonacci Entry Points.* (Parts One and Two). San Jose, Calif.: The Fibonacci Association, 1965.
4. G. T. Hairullin. "Certain Properties of Fibonacci Numbers." *Izv. Vyss. Ucebu. Zaved Matematika* (Russia) 4 (1971):96-101; *Math. Reviews* 44.349.
5. J. H. Halton. "On the Divisibility Properties of Fibonacci Numbers." *The Fibonacci Quarterly* 4, No. 3 (1966):217-40.

6. V. E. Hoggatt, Jr. *Fibonacci and Lucas Numbers*. Boston: Houghton Mifflin, 1969; Santa Clara, Calif.: The Fibonacci Association, 1980.
7. G. Kern-Isberner & G. Rosenberger. "Über Diskretheitsbedingungen und die diophantische Gleichung $ax^2 + by^2 + cz^2 = dxyz$." *Archiv der Math.* 34 (1980):481-93.
8. G. Rosenberger. "Uber Tschebyscheff-Polynome, Nicht-Kongruenzuntergruppen der Modulgruppe und Fibonacci-Zahlen." *Math. Ann.* 246 (1980):193-203.
9. L. Somer. "The Divisibility Properties of Primary Lucas Recurrences with Respect to Primes." *The Fibonacci Quarterly* 18, No. 4 (1980):316-34.

◆◇◆◇◆

LETTER TO THE EDITOR

JOHN BRILLHART
July 14, 1983

In the February 1983 issue of this Journal, D. H. and Emma Lehmer introduced a set of polynomials and, among other things, derived a partial formula for the discriminant of those polynomials (Vol. 21, no. 1, p. 64). I am writing to send you the complete formula; namely,

$$D(P_n(x)) = 5^{n-1}n^{2n-4}F_n^{2n-4},$$

where F_n is the nth Fibonacci number. This formula was derived using the Lehmers' relationship

$$(x^2 - x - 1)P_n(x) = x^{2n} - L_n x^n + (-1)^n,$$

where L_n is the Lucas number. Central to this standard derivation is the nice formula by Phyllis Lefton published in the December 1982 issue of this Journal (Vol. 20, no. 4, pp. 363-65) for the discriminant of a trinomial.

The entries in the Lehmers' paper for $D(P_4(x))$ and $D(P_6(x))$ should be corrected to read

$$2^8 \cdot 3^4 \cdot 5^3 \quad \text{and} \quad 2^{32} \cdot 3^8 \cdot 5^5,$$

respectively.

◆◇◆◇◆