THE NUMBER FIELD $Q(\sqrt{5})$ AND THE FIBONACCI NUMBERS

FRED DODD
University of South Alabama, Mobile, AL 36688
(Submitted August 1982)

1. INTRODUCTION

The set of algebraic integers (hereinafter called integers) of the quadratic number field $Q(\sqrt{5})$ is given by

$$Z(\omega) = \{a + b\omega : a, b \in Z\},$$

where $\omega = \frac{1}{2}(1 + \sqrt{5})$. It is well known that $Z(\omega)$ is a Euclidean domain [6, pp. 214-15], and that the units of $Z(\omega)$ are given by $\pm\omega^n$, where $n \in Z$ [6, p. 221].

The Binet formula

$$F_n = (\omega^n - \overline{\omega}^n)/(\omega - \overline{\omega}) = (\omega^n - \overline{\omega}^n)/\sqrt{5},$$

where $\overline{\omega} = \frac{1}{2}(1 - \sqrt{5})$ is the conjugate of ω, expresses the n^{th} Fibonacci number in terms of the unit ω. Simiarly, the n^{th} Lucas number is given by $L_n = \omega^n + \overline{\omega}^n$. Also, an elementary induction argument using the result $\omega^2 = \omega + 1$ shows that $\omega^n = F_{n-1} + F_n\omega$ for $n \geqslant 1$. These results suggest that the arithmetic theory of $Z(\omega)$ can be a powerful tool in the investigation of the arithmetical properties of the Fibonacci and Lucas numbers. This is indeed the case, and the articles by Carlitz [4], Lind [10], and Lagarias & Weisser [9] utilize $Z(\omega)$ on a limited scale. In this paper, I further document the utility of $Z(\omega)$ by deriving many of the familiar divisibility properties of the Fibonacci numbers using the arithmetic theory of $Z(\omega)$. Much of the development has been adapted from pages 164-174 of my doctoral dissertation [5], which gives a comprehensive treatment of number theory in $Z(\omega)$.

2. CONVENTIONS AND PRELIMINARIES

We assume it is known that $Z(\omega)$ is a Euclidean domain and that the units of $Z(\omega)$ are given by $\pm\omega^n$. In the proof of Theorem 5, we use some results from quadratic residue theory. Apart from this, only the first notions of elementary number theory are taken for granted.

Throughout this paper, lower case Latin letters denote rational integers (elements of Z), and lower case Greek letters denote elements of $Z(\omega)$. The Fibonacci number F_n is denoted by $F(n)$, and n is called the index of the Fibonacci number $F(n)$. Also, p and q denote rational primes; and m, n, and r denote positive rational integers. A greatest common divisor of α and β is denoted by $\text{GCD}(\alpha, \beta)$. Of course, $\text{GCD}(\alpha, \beta)$ is unique up to associates. We continue to use $\gcd(a, b)$ in the sense of rational integer theory; that is, $\gcd(a, b)$ is the unique largest positive rational integer that divides both a and b. We say that α and β are congruent modulo μ, and write $\alpha \equiv \beta \pmod{\mu}$, provided $\mu \mid (\alpha - \beta)$; that is, $\alpha - \beta = \gamma\mu$ for some γ. We continue to use $a \equiv b \pmod{m}$ in the traditional rational integer sense. In the present setting this notation is a bit superfluous since $a \equiv b \pmod{m}$ if and only if $a \equiv b \pmod{m}$. As in rational integer theory, $\alpha + \gamma \equiv \beta + \delta \pmod{\mu}$ and $\alpha\gamma \equiv \beta\delta \pmod{\mu}$ whenever $\alpha \equiv \beta \pmod{\mu}$ and $\gamma \equiv \delta \pmod{\mu}$. Finally, it is clear that $m \mid (c + d\omega)$ in the sense of $Z(\omega)$ if and only if $m \mid c$ and $m \mid d$ in the sense of Z.

3. SIMPLEST DIVISIBILITY PROPERTIES

Our first efforts will be directed toward establishing the classic results listed in Theorem 4. The reader is no doubt familiar with the standard proofs such as found in [6, pp. 148-49] and [11, pp. 29-32]. The attack here is different: An arithmetical function $V(n)$ with values in $Z(\omega)$ and closely related to $F(n)$ is introduced. This function will be shown to have properties analogous to those of $F(n)$ in Theorem 4. Theorem 4 will than follow as a simple corollary.

Definition 1: $V(n) = \omega^{2n} - (-1)^n$.

Theorem 1: $V(n) = \sqrt{5}\omega^n F(n)$.

Proof: By the Binet formula, we have

$$\sqrt{5}\omega^n F(n) = \omega^n(\omega^n - \overline{\omega}^n) = \omega^{2n} - (\omega\overline{\omega})^n = \omega^{2n} - (-1)^n = V(n). \quad \text{Q.E.D.}$$

Theorem 2: If $m|n$, then $V(m)\,|\,V(n)$.

Proof: Let $\alpha = \omega^{2m}$, $\beta = (-1)^m$, and $n = mt$, so that

$$V(m) = \alpha - \beta \quad \text{and} \quad V(n) = \alpha^t - \beta^t.$$

Then $\gamma = \alpha^{t-1} + \alpha^{t-2}\beta + \cdots + \beta^{t-1}$ is an integer and

$$V(n) = \alpha^t - \beta^t = (\alpha - \beta)\gamma = V(m) \cdot \gamma.$$

Thus $V(m)\,|\,V(n)$. Q.E.D.

Lemma 1: If $\omega^{2n} \equiv (-1)^n \pmod{\mu}$, then $\omega^{2na} \equiv (-1)^{na} \pmod{\mu}$ for any rational integer a.

Proof: If $a \geqslant 0$, the result is immediate. If $a < 0$, $\omega^{-2na} \equiv (-1)^{-na} \pmod{\mu}$. Multiplying both sides of the last congruence by the integer $(-1)^{na}\omega^{2na}$, we obtain $\omega^{2na} \equiv (-1)^{na} \pmod{\mu}$. Q.E.D.

Theorem 3: If $d = \gcd(n, m)$, then $\mathrm{GCD}(V(n), V(m)) = V(d)$.

Proof: Let $\delta = \mathrm{GCD}(V(n), V(m))$. Since $d = \gcd(n, m)$, there exist a and b such that $d = ma + nb$. Now $V(m) \equiv 0 \pmod{\delta}$, so that $\omega^{2m} \equiv (-1)^m \pmod{\delta}$. Similarly, $\omega^{2n} \equiv (-1)^n \pmod{\delta}$. Thus, by Lemma 1,

$$\omega^{2ma} \equiv (-1)^{ma} \pmod{\delta} \quad \text{and} \quad \omega^{2nb} \equiv (-1)^{nb} \pmod{\delta}.$$

Accordingly, $\omega^{2ma+2nb} \equiv (-1)^{ma+nb} \pmod{\delta}$, and since $d = ma + nb$, $\omega^{2d} \equiv (-1)^d \pmod{\delta}$. Consequently, $V(d) = \omega^{2d} - (-1)^d \equiv 0 \pmod{\delta}$; that is, $\delta\,|\,V(d)$. Conversely, since $d|n$ and $d|m$, $V(d)\,|\,V(n)$ and $V(d)\,|\,V(m)$ by Theorem 2; and so $V(d)\,|\,\delta$. We thus conclude that $\delta = V(d)$ (up to associates). Q.E.D.

Theorem 4: (i) If $m|n$, then $F(m)\,|\,F(n)$.
(ii) If $d = \gcd(m, n)$, then $\gcd(F(m), F(n)) = F(d)$. In particular, if $\gcd(m, n) = 1$, then $\gcd(F(m), F(n)) = 1$.

(iii) If $\gcd(n, m) = 1$, then $F(m) \cdot F(n) \mid F(mn)$.
(iv) If $m > 2$, then $m \mid n$ if and only if $F(m) \mid F(n)$.

Proof: If $m \mid n$, then $V(m) \mid V(n)$ by Theorem 2. Thus, by Theorem 1, $\sqrt{5}\omega^m F(m)$ divides $\sqrt{5}\omega^n F(n)$; and since ω is a unit, $F(m) \mid F(n)$. This establishes (i). By Theorems 1 and 3, we have

$$\sqrt{5}\omega^d F(d) = V(d) = \mathrm{GCD}(V(m), V(n)) = \mathrm{GCD}(\sqrt{5}\omega^m F(m), \sqrt{5}\omega^n F(n))$$
$$= \sqrt{5}\mathrm{GCD}(F(m), F(n)).$$

Thus $F(d) = \mathrm{GCD}(F(m), F(n))$, and so $F(d) = \gcd(F(m), F(n))$. Consequently, (ii) is true. Now (iii) follows from (i) and (ii), because $F(m) \mid F(mn)$, $F(n) \mid F(mn)$, and $\gcd(F(m), F(n)) = 1$. Half of (iv) follows from (i). Suppose $F(m) \mid F(n)$. Then by (ii) we have $F(m) = \gcd(F(m), F(n)) = F(d)$, where $d = \gcd(m, n)$. Thus $F(m) = F(d)$; and if $m > 2$, we have $m = d = \gcd(m, n)$, so that $m \mid n$. Q.E.D.

Corollary 1: $\gcd(F(n), F(n + 1)) = 1$.

Proof: We have $\gcd(n, n + 1) = 1$, and so, by Theorem 4(ii),

$$\gcd(F(n), F(n + 1)) = F(1) = 1. \quad \text{Q.E.D.}$$

4. LAW OF APPARITION AND RELATED RESULTS

If $m > 0$ is given, then a classical result states that m divides some Fibonacci number having positive index not exceeding m^2 [7, p. 44]. In this section we deal with various aspects of this problem. The key results we need from the arithmetic theory of $Z(\omega)$ are found in Theorems 5 and 6. Theorem 5 and its proof is a special case of Theorem 258 in Hardy and Wright [6, pp. 222-23]. Theorem 6, although trivial to prove, will be used many times in the remainder of this paper.

Theorem 5: If $p \equiv \pm 2 \pmod 5$ and $q \equiv \pm 1 \pmod 5$, then

$$\text{(i)} \quad \omega^{p+1} \equiv -1 \ (\mathrm{MOD}\ p) \quad \text{and} \quad \text{(ii)} \quad \omega^{q-1} \equiv 1 \ (\mathrm{MOD}\ q).$$

Proof: Since $\omega^2 - \overline{\omega} = \omega + 1 - (1 - \omega) = 2\omega$, then $\omega^2 \equiv \overline{\omega} \pmod 2$. Accordingly, $\omega^3 \equiv \omega\overline{\omega} = -1 \pmod 2$ and the result is true for $p = 2$.

Now let $t \neq 5$ be an odd rational prime. Since $2^t \equiv 2 \pmod t$, by Fermat's theorem for rational integers, we have

$$2\omega^t \equiv (2\omega)^t = (1 + \sqrt{5})^t \equiv 1 + 5^{\frac{1}{2}(t-1)}\sqrt{5} \ (\mathrm{MOD}\ t).$$

By Euler's criterion for quadratic residues, $5^{\frac{1}{2}(t-1)} \equiv (5 \mid t) \pmod t$. Therefore, $2\omega^t \equiv 1 + (5 \mid t)\sqrt{5} \ (\mathrm{MOD}\ t)$. By quadratic reciprocity, $(5 \mid p) = (p \mid 5) = -1$ and $(5 \mid q) = (q \mid 5) = 1$. Thus

$$2\omega^p \equiv 1 - \sqrt{5} = 2\overline{\omega} \ (\mathrm{MOD}\ p) \quad \text{and} \quad 2\omega^q \equiv 1 + \sqrt{5} = 2\omega \ (\mathrm{MOD}\ q).$$

By cancellation, $\omega^p \equiv \overline{\omega} \pmod p$ and $\omega^q \equiv \omega \pmod q$. Thus

$$\omega^{p+1} \equiv \omega\overline{\omega} = -1 \ (\mathrm{MOD}\ p) \quad \text{and} \quad \omega^{q-1} = \omega^{-1}\omega^q \equiv \omega^{-1}\omega = 1 \ (\mathrm{MOD}\ q). \quad \text{Q.E.D.}$$

Theorem 6: We have that $m|F(n)$ if and only if ω^n is congruent modulo m to a rational integer. Moreover, if $m|F(n)$, then $\omega^n \equiv F(n-1) \pmod{m}$.

Proof: If $m|F(n)$, then

$$\omega^n = F(n-1) + F(n)\omega \equiv F(n-1) \pmod{m}.$$

Conversely, if $\omega^n \equiv \alpha \pmod{m}$, then $\overline{\omega}^n \equiv \alpha \pmod{m}$. Thus, we have $\omega^n - \overline{\omega}^n \equiv 0 \pmod{m}$; and since

$$\omega^n - \overline{\omega}^n = \sqrt{5}F(n) = (-1 + 2\omega)F(n) = -F(n) + 2F(n)\omega,$$

it follows that $m|F(n)$. Q.E.D.

Theorem 7 (Law of Apparition): If $p \equiv \pm 2 \pmod{5}$ and $q \equiv \pm 1 \pmod{5}$, then

$$\text{(i)}\quad p|F(p+1), \quad \text{(ii)}\quad q|F(q-1), \text{ and } \quad \text{(iii)}\quad 5|F(5).$$

Proof: By Theorem 5, $\omega^{p+1} \equiv -1 \pmod{p}$ and $\omega^{q-1} \equiv 1 \pmod{q}$. Thus, by Theorem 6, $p|F(p+1)$ and $q|F(q-1)$. Assertion (iii) is immediate, because $F(5) = 5$. Q.E.D.

Theorem 8: If $p^r|F(n)$, then $p^{r+1}|F(np)$.

Proof: Since $p^r|F(n)$, $\omega^n \equiv \alpha \pmod{p^r}$ by Theorem 6. Thus $\omega^n = \alpha + p^r\alpha$ and so

$$\omega^{np} = (\alpha + p^r\alpha)^p \equiv \alpha^p + p\alpha^{p-1}p^r\alpha \equiv \alpha^p \pmod{p^{r+1}}.$$

It therefore follows from Theorem 6 that $p^{r+1}|F(np)$. Q.E.D.

Theorem 9: If $p|F(n)$, then $p^r|F(p^{r-1}n)$.

Proof: The proof is by induction on r. By hypothesis, the result holds for $r = 1$; and if $p^r|F(p^{r-1}n)$, then $p^{r+1}|F(p^rn)$ by Theorem 8. Q.E.D.

Theorem 10: If $p \equiv \pm 2 \pmod{5}$ and $q \equiv \pm 1 \pmod{5}$, then

$$\text{(i)}\quad p^r|F(p^{r-1}(p+1)), \quad \text{(ii)}\quad q^r|F(q^{r-1}(q-1)), \quad \text{(iii)}\quad 5^r|F(5^r).$$

Proof: Immediate from Theorems 7 and 9.

Definition 2: If $p \equiv \pm 2 \pmod{5}$ and $q \equiv \pm 1 \pmod{5}$, then

$$T(1) = 1, \ T(p^r) = p^{r-1}(p+1), \ T(q^r) = q^{r-1}(q-1), \ T(5^r) = 5^r;$$

and if m has the rational prime decomposition $m = p_1^{e_1}p_2^{e_2} \cdots p_s^{e_s}$, then

$$T(m) = \operatorname{lcm}(T(p_1^{e_1}), T(p_2^{e_2}), \ldots, T(p_s^{e_s})).$$

Theorem 11: We have $m|F(T(m))$.

Proof: The result is certainly true if $m = 1$. If $m > 1$, then let m have the rational prime decomposition

$$m = p_1^{e_1}p_2^{e_2} \cdots p_s^{e_s}.$$

Since $T(p_i^{e_i})$ divides $T(m)$, $F(T(p_i^{e_i}))$ divides $F(T(m))$ by Theorem 4(i). Also $p_i^{e_i}$ divides $F(T(p_i^{e_i}))$ by Theorem 10 and Definition 2. Thus, $p_i^{e_i}$ divides $F(T(m))$,

And since the $p_i^{e_i}$ are pairwise relatively prime, m divides $F(T(m))$. Q.E.D.

The result mentioned at the beginning of this section is an immediate consequence of Theorem 11, since it is clear that $1 \leq T(m) \leq m^2$. Theorem 11 is a stronger result in the sense that it exhibits an easily calculated positive index n for which $m|F(n)$.

5. RANK OF APPARITION

Given $m > 0$, it is natural to ask for the smallest $t > 0$ for which $m|F(t)$. We might take $T(m)$ as a tentative guess for t. This guess may not be correct ($T(17) = 18$ and $17|F(9)$), but as we shall presently see in Theorem 13, $t|T(m)$.

Definition 3: The rank of apparition of $m > 0$, denoted by $R(m)$, is the smallest $t > 0$ such that $m|F(t)$. We also say that the index t is the point of entry of m in the Fibonacci numbers.

Tables of $R(p)$ are readily available. Brousseau [1] gives $R(p)$ for each rational prime $p \leq 269$, while [2] does the same for $p < 48{,}179$ and [3] does for $48{,}179 \leq p < 100{,}000$. Jarden, in [8], gives $R(p)$ for each rational prime $p < 1512$. The following theorem gives a concise formulation of $R(m)$ in terms of the structure of $Z(\omega)$.

Theorem 12: $R(m)$ is the smallest $t > 0$ such that ω^t is congruent modulo m to a rational integer.

Proof: Immediate from Theorem 6. Q.E.D.

It should be noted that the period of m in the Fibonacci numbers also has a concise formulation in $Z(\omega)$. Recall that the period of m in the Fibonacci numbers is the smallest $t > 0$ such that $F(t - 1) \equiv 1 \pmod{m}$ and $F(t) \equiv 0 \pmod{m}$. Thus, since $\omega^t = F(t - 1) + F(t)\omega$, it follows that the period of m in the Fibonacci numbers is the smallest $t > 0$ such that $\omega^t \equiv 1 \pmod{m}$.

The following trivial lemma paves the way for Theorem 13, the main result of this section.

Lemma 2: The integer $c + d\omega$ is congruent modulo m to a rational integer if and only if $m|d$.

Proof: If $m|d$, then $c + d\omega \equiv c \pmod{m}$. Conversely, if $c + d\omega \equiv a \pmod{m}$, then $m|(c - a)$ and $m|d$. Q.E.D.

Theorem 13: We have that $m|F(n)$ if and only if $R(m)|n$.

Proof: Let $t = R(m)$. First, suppose that $t|n$. Then, by Theorem 4(i), we have $F(t)|F(n)$; and since $m|F(t)$, it follows that $m|F(n)$. Conversely, suppose that $m|F(n)$. Then $\omega^n \equiv b \pmod{m}$ by Theorem 6. Since $n \geq t$, then $n = st + x$, where $s > 0$ and $0 \leq x < t$. Thus, as $\omega^t \equiv a \pmod{m}$ for some a with $\gcd(a, m) = 1$ (Theorem 6), we have $b \equiv \omega^n = \omega^{st+x} \equiv a^s\omega^x \pmod{m}$. Suppose $x \neq 0$. Then $\omega^x = c + d\omega$ and $m \nmid d$. [For, if $m|d$, we would have $\omega^x \equiv c \pmod{m}$ by Lemma 2, and so $m|F(x)$, a contradiction to the minimality of t.] Thus, $b \equiv ca^s + da^s\omega \pmod{m}$. This is impossible by Lemma 2 [$\gcd(a, m) = 1$ and $m \nmid d$; thus $m \nmid da^s$.] Accordingly, $x = 0$, and so $t|n$. Q.E.D.

6. LAW OF REPETITION

We now direct our efforts to establishing the law of repetition (Theorem 15). Along the way, we will establish Theorem 14 and Lemma 3. Theorem 14 is an important result in its own right, whereas Lemma 3 is instrumental in proving the law of repetition. The proof of Lemma 3 will be the last use of the arithmetic theory of $Z(\omega)$ in this paper.

Definition 4: By $p^r \| n$, we mean that $p^r | n$ and $p^{r+1} \nmid n$.

Theorem 14: If $p^r \| F(n)$, then $p^{r+1} | F(nm)$ if and only if $p | m$.

Proof: Suppose $p | m$. We have that $p^{r+1} | F(np)$ by Theorem 8; and since $np | mn$, it follows from Theorem 4(i) that $F(np) | F(nm)$. Now suppose that $p^{r+1} | F(nm)$. Set $a = F(n-1)$ and $bp^r = F(n)$. Since $p^r \| F(n)$, it follows that $\gcd(b, p) = 1$; and $\gcd(a, p) = 1$, since $F(n-1)$ and $F(n)$ are relatively prime. Therefore, $\gcd(ab, p) = 1$. Also,

$$\omega^{nm} = (a + bp^r\omega)^m \equiv a^m + ma^{m-1}bp^r\omega \pmod{p^{r+1}}.$$

Now $p^{r+1} | F(nm)$, and so, by Theorem 6, we have

$$a^m + ma^{m-1}bp^r\omega \equiv c \pmod{p^{r+1}}.$$

But, by Lemma 2, this means that $p | ma^{m-1}b$; and since $\gcd(ab, p) = 1$, it follows that $p | m$. Q.E.D.

Lemma 3: If $p^r \| F(n)$ and $\gcd(m, p) = 1$, then

$$p^{r+1} | F(nmp),$$

and if $p^r \neq 2$, then

$$p^{r+1} \| F(nmp).$$

Proof: Since $n | nm$, then $F(n) | F(nm)$, and so $p^r | F(nm)$. Thus, $p^{r+1} | F(nmp)$, by Theorem 8. Also, since $\gcd(m, p) = 1$, we have $p \nmid m$, so that $p^{r+1} \nmid F(nm)$, by Theorem 14. Accordingly, $p^r \| F(nm)$. Let $x = nm$. Then we have $p^r \| F(x)$, and we are to show that, if $p^r \neq 2$, then $p^{r+1} \| F(xp)$. Of course, we already know that $p^{r+1} | F(xp)$, and so it only remains to show that $p^{r+2} \nmid F(xp)$.

Suppose first that $p > 2$. Set $a = F(x-1)$ and $bp^r = F(x)$. As in the proof of Theorem 14, we have $\gcd(ab, p) = 1$. Also,

$$\omega^{px} = (a + bp^r\omega)^p = a^p + p^{r+1}a^{p-1}b\omega + \alpha p^{r+2}.$$

Thus,

$$\omega^{px} \equiv a^p + p^{r+1}a^{p-1}b\omega \pmod{p^{r+2}},$$

and since $p^{r+2} \nmid p^{r+1}a^{p-1}b$, it follows that ω^{px} is not congruent modulo p^{r+2} to a rational integer (Lemma 2). Therefore, by Theorem 6, $p^{r+2} \nmid F(xp)$.

The proof for the exceptional case $p = 2$, $r > 1$, is exactly the same. (The condition $r > 1$ is needed to obtain the term αp^{r+2}.) Q.E.D.

Theorem 15 (Law of Repetition): If $p^r \| F(n)$ and $\gcd(m, p) = 1$, then, for any $k \geqslant 0$, $p^{r+k} | F(nmp^k)$, and if $p^r \neq 2$, $p^{r+k} \| F(nmp^k)$.

Proof: Straightforward induction on k using Theorem 8 and Lemma 3. Q.E.D.

7. FURTHER DIVISIBILITY RESULTS

We conclude this article by listing in Theorems 16-20 additional well-known divisibility results which readily follow from Theorems 13-15. Since no additional use of the arithmetic theory of $Z(\omega)$ is needed, the proofs are left to the reader.

Theorem 16: If $p \neq 2$, $t = R(p)$, $p^r \| F(t)$, and $k \geqslant 0$, then $p^{r+k} \| F(n)$ if and only if $n = tmp^k$, where $\gcd(m, p) = 1$.

Theorem 17: (i) $2 \| F(n)$ if and only if $n = 3m$, where $\gcd(m, 2) = 1$.
(ii) If $k \geqslant 0$, then $2^{3+k} \| F(n)$ if and only if $n = 2^{k+1} \cdot 3 \cdot m$, where $\gcd(m, 2) = 1$.

Theorem 18: If $p \neq 2$, $t = R(p)$, and $p^r \| F(t)$, then

$$R(p^n) = t \cdot p^{\max(0, n-r)} \quad \text{and} \quad p^{r+\max(0, n-r)} \| F(R(p^n)).$$

Theorem 19:

$$R(2^n) = \begin{cases} 3, & n = 1 \\ 2 \cdot 3, & n = 2. \\ 2^{n-2} \cdot 3, & n \geqslant 3 \end{cases}$$

Furthermore, $2 \| F(3)$, $2^3 \| F(2 \cdot 3)$, and $2^n \| F(2^{n-2} \cdot 3)$ for $n \geqslant 3$.

Theorem 20: If $m = p_1^{e_1} p_2^{e_2} \ldots p_s^{e_s}$, then

$$R(m) = \operatorname{lcm}(R(p_1^{e_1}), \ldots, R(p_s^{e_s})).$$

REFERENCES

1. Brother Alfred Brousseau. *An Introduction to Fibonacci Discovery.* Santa Clara, Calif.: The Fibonacci Association, 1965.
2. Brother Alfred Brousseau, ed. *Tables of Fibonacci Entry Points, Part One.* Santa Clara, Calif.: The Fibonacci Association, 1965.
3. Brother Alfred Brousseau. *An Introduction to Fibonacci Entry Points, Part Two.* Santa Clara, Calif: The Fibonacci Assocation, 1965.
4. L. Carlitz. "A Note on Fibonacci Numbers." *The Fibonacci Quarterly* 2, no. 1 (1964):15-28.
5. F. Dodd. "Number Theory in the Integral Domain $Z(\frac{1}{2} + \frac{1}{2}\sqrt{5})$." Doctor of Arts dissertation, University of Northern Colorado, Greeley, Colorado, 1981.
6. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers.* 5th ed. London: Oxford University Press, 1979.
7. Verner E. Hoggatt, Jr. *Fibonacci and Lucas Numbers.* Boston: Houghton Mifflin, 1969, Rpt. The Fibonacci Association, 1980.
8. Dov Jarden. *Recurring Sequences.* 3rd ed. Jerusalem: Riveon Lematematika, 1973.
9. J. C. Lagarias & D. P. Weisser. "Fibonacci and Lucas Cubes." *The Fibonacci Quarterly* 19, no. 1 (1981):39-43.
10. D. A. Lind. "The Quadratic Field $Q(\sqrt{5})$ and a Certain Diophantine Equation." *The Fibonacci Quarterly* 6, no. 3 (1968):86-93.
11. N. N. Vorob'ev. *Fibonacci Numbers.* New York: Blaisdell, 1961.

◆◇◆◇◆