THE QUADRATIC FIELD $Q(\sqrt{5})$ AND A CERTAIN DIOPHANTINE EQUATION

D.A.Lind,

University of Virginia, Charlottesville, Va.

1. INTRODUCTION

We establish here a characterization of the Fibonacci and Lucas numbers while determining the units of the quadratic field extension $Q(\sqrt{5})$ of the rational field Q. Using an appropriate norm on $Q(\sqrt{5})$, we also find all solutions to the Diophantine equation $x^2 - 5y^2 = \pm 4$ and solve a certain binomial coefficient equation. Except for the definitions of basic algebraic structures, the treatment is self-contained, and so should also serve as a brief introduction to algebraic number theory. We hope the reader sees the beauty of one branch of mathematics interacting profitably with another, wherein both gain.

For the definitions of group, ring, and field, we refer the reader to [1]. Let u be an element of the field of complex numbers C. We say u is an algebraic number if there is a polynomial

$$(1) \qquad p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \quad (a_i \in Q, \ a_n \neq 0)$$

with coefficients in Q not all zero which is satisfied by u, i.e., such that

$$p(u) = a_n u^n + a_{n-1}u^{n-1} + \cdots + a_1 u + a_0 = 0 .$$

Thus $\sqrt{2}$ and $i = \sqrt{-1}$ are algebraic numbers, while π is not. Among all the polynomials satisfied by u, there is one of least positive degree, say of the form p(x) in (1). Since p(u) = 0 implies $a_n^{-1}p(u) = 0$, we may choose p(x) with leading coefficient 1, i.e., so that p(x) is monic. The monic polynomial of least positive degree satisfied by u is called the minimal polynomial of u. For example, the minimal polynomial of $\frac{1}{2}\sqrt{2}$ is $x^2 - \frac{1}{2}$. The reason we insist that the leading coefficient of p(x) be 1 is that with this provision the minimal polynomial is unique (see [1, Chap. 14]).

An algebraic number is said to be an algebraic integer if its minimal polynomial has integral coefficients. For example, any rational r is an algebraic number (it satisfies $x - r$), but among the rationals only the integers are algebraic integers (the reader should prove this). For this reason the ordinary integers are sometimes referred to as rational integers. An algebraic number $u \neq 0$ is called a unit if both u and u^{-1} are algebraic integers. As an example, -1 and i are units. A unit should be distinguished from the unit (multiplicative identity) element 1 of the field, although the unit element is also a unit.

3. THE QUADRATIC FIELD $Q(\sqrt{5})$

Denote by $Q(\sqrt{5})$ the smallest field contained in the field of real numbers R which contains both Q and $\sqrt{5}$. We first expose the form of the elements in $Q(\sqrt{5})$.

Theorem 1. $Q(\sqrt{5}) = \{r + s\sqrt{5} \mid r, s \in Q\}$.

Proof. Denote the right side in Theorem 1 by S. Then since the elements of S are formed using the field operations from those in Q and $\sqrt{5}$, we have $S \subset Q(\sqrt{5})$. But we claim S is already a field. Clearly it inherits the necessary additive and associative properties from R, and the product of any two elements in S is easily shown to be again in S. Hence we must only show the existence of inverses in S. If $r + s\sqrt{5} \neq 0$, then

$$\frac{1}{r + s\sqrt{5}} = \frac{r - s\sqrt{5}}{r^2 - 5s^2} = \frac{r}{r^2 - 5s^2} - \left(\frac{s}{r^2 - 5s^2}\right)\sqrt{5} \in S .$$

Since $Q(\sqrt{5})$ is the smallest subfield of R containing Q and $\sqrt{5}$, we have $Q(\sqrt{5}) \subset S$. Thus $S = Q(\sqrt{5})$.

Because of the irrationality of $\sqrt{5}$, we note that two elements in $Q(\sqrt{5})$ are equal if and only if they are equal componentwise, i.e., $a + b\sqrt{5} = c + d\sqrt{5}$ for $a, b, c, d \in Q$ if and only if $a = c$ and $b = d$. $Q(\sqrt{5})$ is called a quadratic field because it is formed by adjoining $\sqrt{5}$ to Q, and the minimal polynomial of $\sqrt{5}$ is a quadratic.

We next describe the set $Q_i(\sqrt{5})$ of algebraic integers in R which also occur in $Q(\sqrt{5})$.

Theorem 2. The set $Q_i(\sqrt{5})$ of algebraic integers in $Q(\sqrt{5})$ consists of precisely the numbers $\frac{1}{2}(a + b\sqrt{5})$, where a and b are integers such that $a \equiv b \pmod{2}$.

Proof. Using Theorem 1, any number u in $Q(\sqrt{5})$ may be expressed as $u = (a + b\sqrt{5})/c$, where the integers a, b, and c have no common factor except ±1. We may assume $b \neq 0$ to exclude the trivial case when u is rational. Then the monic polynomial of lowest degree satisfied by u is

$$(2) \qquad p(x) = \left(x - \frac{a + b\sqrt{5}}{c}\right)\left(x - \frac{a - b\sqrt{5}}{c}\right) = x^2 - \left(\frac{2a}{c}\right)x + \frac{a^2 - 5b^2}{c^2} .$$

If u is to be an algebraic integer, then the coefficients $2a/c$ and $(a^2 - 5b^2)/c^2$ must be integers. Thus $4a^2 / c^2$, $(4a^2 - 20b^2)/c^2$, and hence $20b^2/c^2$ must all be integers, so that $c|2a$ and $c^2|20b^2$, where $n|m$ means n divides m. Now any prime factor $p \neq 2$ of c must divide both a and b by the above, contrary to our assumption that a, b, c have no common factor except ±1. Similarly $4|c$ is impossible, so the only choices left are $c = 1$ and $c = 2$.

If $c = 1$, p(x) has integral coefficients and u is an algebraic integer. In this case u has the form $\frac{1}{2}(2a + 2b\sqrt{5})$, and $2a \equiv 2b \equiv 0 \pmod 2$, so the conclusion of the theorem is true. If $c = 2$, then $(a^2 - 5b^2)/c^2 = (a^2 - 5b^2)/4$ is an integer if and only if a and b are either both odd or both even, or equivalently $a \equiv b \pmod 2$. Hence the theorem also holds here, completing the proof.

We remark the $Q_i(\sqrt{5})$ actually forms a ring because it is closed under multiplication. The reader is urged to verify the details.

We next investigate the question of units in $Q(\sqrt{5})$. First note that by definition if u_1 and u_2 are units, then u_1, u_1^{-1}, u_2, u_2^{-1}, $-u_1$ are all in $Q_i(\sqrt{5})$. Using Theorem 2, it is straightforward to verify that then u_1u_2, $(u_1u_2)^{-1}$, $u_1u_2^{-1}$, $(u_1u_2^{-1})^{-1}$, $(-u_1)^{-1}$ are also in $Q_i(\sqrt{5})$. Hence u_1u_2, $u_1u_2^{-1}$, and $-u_1$ are units in $Q(\sqrt{5})$. In particular, if u is a unit, so is u^{-1}.

The Gaussian integers J are the set of complex numbers with integral real and imaginary parts. A useful function from J to the nonnegative integers is the norm defined by $|a + bi| = a^2 + b^2$. This norm is handy because $|xy| = |x||y|$ for $x, y \in J$, so it preserves the multiplicative structure of J. We now introduce an analogous function on $Q_i(\sqrt{5})$. If $u = \frac{1}{2}(a + b\sqrt{5}) \in Q_i(\sqrt{5})$, define the norm of u by

$$N(u) = \tfrac{1}{2}(a + b\sqrt{5})\tfrac{1}{2}(a - b\sqrt{5}) = \tfrac{1}{4}(a^2 - 5b^2) .$$

The reader should verify that $N(u)$ is always an integer (possibly negative), and that $N(u_1u_2) = N(u_1)N(u_2)$ for all $u_1, u_2 \in Q_i(\sqrt{5})$. We use this norm to obtain a characterization of units.

Theorem 3. An element $u \in Q_i(\sqrt{5})$ is a unit if and only if $N(u) = \pm 1$.

Proof. If u is a unit, then $u, u^{-1} \in Q_i(\sqrt{5})$, so that $1 = N(1) = N(uu^{-1}) = N(u)N(u^{-1})$. Since $N(u)$ and $N(u^{-1})$ are integers, $N(u) = \pm 1$. Conversely, if $u = \frac{1}{2}(a + b\sqrt{5}) \in Q_i(\sqrt{5})$ such that $N(u) = \pm 1$, then

$$\tfrac{1}{2}(a + b\sqrt{5})\,\tfrac{1}{2}(a - b\sqrt{5}) = \pm 1 ,$$

so that

$$u^{-1} = \pm\tfrac{1}{2}(a - b\sqrt{5}) \in Q_i(\sqrt{5})$$

by Theorem 2. Thus u is a unit.

Using the norm function on $Q_i(\sqrt{5})$ and recalling that a unit in $Q(\sqrt{5})$ must already be in $Q_i(\sqrt{5})$, we can obtain a complete accounting of the units in $Q(\sqrt{5})$. Let $\alpha = (1 + \sqrt{5})/2 \in Q_i(\sqrt{5})$. Then $N(\alpha) = -1$, so by Theorem 3 α is a unit in $Q(\sqrt{5})$. By the above remarks we therefore know that $\pm\alpha$, $\pm\alpha^2, \pm\alpha^3, \cdots, \pm 1, \pm\alpha^{-1}, \pm x^{-2}, \cdots$ are units in $Q(\sqrt{5})$. Thus in contrast with the Gaussian integers J, where the only units are $\pm 1, \pm i$, in $Q(\sqrt{5})$ there are units of either sign as large or as small as we please.

Theorem 4. The numbers

$$(3) \qquad \pm\alpha^{n}, \ \pm\alpha^{-n} \qquad (n = 0, 1, 2, \cdots)$$

are the only units in $Q(\sqrt{5})$.

Proof. We first prove there is no unit between 1 and α. Suppose that there is a unit $u \in Q_i(\sqrt{5})$ such that $1 < u < \alpha$. By Theorem 2, $u = \frac{1}{2}(x + y\sqrt{5})$, where x and y are integers. Then by Theorem 3

$$\pm 1 = N(u) = \frac{x^2 - 5y^2}{4} = \left(\frac{x + y\sqrt{5}}{2}\right)\left(\frac{x - y\sqrt{5}}{2}\right),$$

so that using $1 < u$ we find

$$-\tfrac{1}{2}(x + y\sqrt{5}) < -1 \le \tfrac{1}{2}(x + y\sqrt{5})\tfrac{1}{2}(x - y\sqrt{5}) \le 1 < \tfrac{1}{2}(x + y\sqrt{5}) \ .$$

Dividing by $u \neq 0$ yields

$$-1 < \tfrac{1}{2}(x - y\sqrt{5}) < 1 \ . \tag{4}$$

Adding (4) to $1 < u < \alpha$ gives

$$0 < x < 1 + \alpha,$$

showing that $x = 1$ or 2. But in either case there is no integer y such that $1 < u < \alpha$ holds. This contradiction shows there is no unit between 1 and α.

Now to finish the proof. Suppose $u \neq 0$ is a unit, where we may assume u is positive since $-u$ is also a unit. Then either $u = \alpha^n$, or there is an integer n such that $\alpha^n < u < \alpha^{n+1}$. Now α^{-n} is a unit, implying $\alpha^{-n}u$ also is. But then $1 < \alpha^{-n}u < \alpha$, which was shown impossible in the first part of the proof. Hence the only units in $Q(\sqrt{5})$ are given in (3).

We now use Theorem 4 to give a characterization of Fibonacci and Lucas numbers. But we first need,

Theorem 5. Define the Fibonacci numbers F_n by $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_{n+1} + F_n$, and the Lucas numbers L_n by $L_0 = 2$, $L_1 = 1$, $L_{n+2} = L_{n+1} + L_n$. Then

$$\alpha^n = \tfrac{1}{2}(L_n + F_n\sqrt{5}) \ .$$

Proof. We establish this by induction. It is certainly true for $n = 0, 1$. If it is valid for $n = k$, $k + 1$, simply adding the corresponding equations together with the fact that $\alpha^{k+2} = \alpha^{k+1} + \alpha^k$ shows it holds for $n = k + 2$, completing the induction step and the proof.

Theorem 6. The algebraic number $\frac{1}{2}(a + b\sqrt{5}) \in Q(\sqrt{5})$ is a unit if and only if $a = L_n$ and $b = F_n$ for some integer n.

Proof. This is a combination of Theorems 4 and 5.

Thus we have characterized the Fibonacci and Lucas numbers in terms of the units in $Q(\sqrt{5})$. We note in passing that since α^n is a unit of $Q(\sqrt{5})$, Theorem 2 implies $F_n \equiv L_n \pmod{2}$.

An application of these properties of $Q(\sqrt{5})$ to prove the converse of a familiar property of the Fibonacci numbers has been given by Carlitz [2]. This type of development is capable of generalization to $Q(\sqrt{d})$, where d may be assumed to be a squarefree integer. One striking fact is that the analogue of unique factorization of elements into powers of irreducible (prime) elements holds for only a finite number of d ($d = 5$ is one of them). For further information about this, we refer the reader to [3; Chap. 15] for a number theoretic approach, and to [1; Chap. 14] for an algebraic one.

4. THE SOLUTION OF $x^2 - 5y^2 = \pm 4$

We show here how the solutions of the Diophantine equation $x^2 - 5y^2 = \pm 4$ may be easily obtained as a byproduct of the preceding algebraic material. Note that $N(\alpha) = -1$, so that $N(\alpha^n) = (-1)^n$. Then if $u \in Q_i(\sqrt{5})$, $N(u) = 1$ if and only if $u = \alpha^{2n}$, and $N(u) = -1$. if and only if $u = \alpha^{2n+1}$ for some integer n. This observation leads to the

Theorem 7. (i) All rational integral solutions of $x^2 - 5y^2 = 4$ are given by $x = L_{2n}$, $y = F_{2n}$, and (ii) all of $x^2 - 5y^2 = -4$ by $x = L_{2n+1}$, $y = F_{2n+1}$ $(n = 0, \pm 1, \pm 2, \cdots)$.

Proof. (i) Since $N(\alpha^{2n}) = 1$, Theorem 5 shows that the purported solutions actually satisfy $x^2 - 5y^2 = 4$. Conversely, if $x^2 - 5y^2 = 4$, then $x \equiv y \pmod 2$ and $N[\frac{1}{2}(x + y\sqrt{5})] = 1$. By the preceeding remarks, $\frac{1}{2}(x + y\sqrt{5}) = \alpha^{2n}$ for some n, so that by Theorem 5 $x = L_{2n}$, $y = F_{2n}$, showing that these are all the solutions.

(ii) As in (i), $N(\alpha^{2n+1}) = -1$ and Theorem 5 show that $x = L_{2n+1}$, $y = F_{2n+1}$ are actually solutions. On the other hand, if $x^2 - 5y^2 = -4$, then $x \equiv y \pmod 2$ and $N[\frac{1}{2}(x + y\sqrt{5})] = -1$. Then $\frac{1}{2}(x + y\sqrt{5}) = \alpha^{2n+1}$ for some n, so by Theorem 5 $x = L_{2n+1}$, $y = F_{2n+1}$, completing the proof.

We remark that Theorem 7 was proved by Long and Jordan [4] by using the classical theory of the Pell equation, from which the result follows easily. Theorem 7 also provides a characterization of Fibonacci and Lucas numbers analogous to Theorem 6, but in terms of a Diophantine equation.

5. THE SOLUTION OF A CERTAIN BINOMIAL COEFFICIENT EQUATION

We shall use the preceding results to solve completely the seemingly unrelated binomial coefficient equation,

$$\binom{n}{k} = \binom{n-1}{k+1}. \tag{5}$$

For example, the three solutions of (5) with smallest n are

$$\binom{2}{0} = \binom{1}{1} = 1, \binom{15}{5} = \binom{14}{6} = 3003, \binom{104}{39} = \binom{103}{40}. \tag{6}$$

First note that by cancelling common factors, (5) is equivalent to

$$n(k+1) = (n-k)(n-k-1) \ ,$$

or

$$k^2 + (1 - 3n)k + n^2 - 2n = 0 \ .$$

This quadratic in k has a solution in integers if and only if its discriminant $5n^2 + 2n + 1$ is a perfect square, say

$$5n^2 + 2n + 1 = t^2 \ .$$

Then

$$25n^2 + 10n + 1 = 5t^2 - 5 + 1,$$

so that

$$(5n+1)^2 - 5t^2 = -4 \ , \tag{7}$$

which is the form of the Diophantine equation which we solved in the previous section. Then by (ii) of Theorem 7, (7) has an integral solution if and only if

$x = L_{2r+1}$, $y = F_{2r+1}$, and $x \equiv 1 \pmod 5$, the last condition being imposed so that n is an integer. Now it is easy to verify that $L_{2r+1} \equiv 1 \pmod 5$ if and only if r is even, say $r = 2s$, so all solutions of (7) are given by

$$n = \frac{L_{4s+1} - 1}{5}, \quad t = F_{4s+1} .$$

Using the Binet form for Fibonacci and Lucas numbers, we have

$$n = \frac{L_{4s+1} - 1}{5} = F_{2s}F_{2s+1} .$$

Also,

$$k = \frac{3n - 1 - t}{2} = \tfrac{1}{2}(3F_{2s}F_{2s+1} - 1 - F_{4s+1}) = F_{2s-2}F_{2s+1} .$$

Hence all solutions of our original equation (5) are given by

$$n = F_{2s}F_{2s+1} , \quad k = F_{2s-2}F_{2s+1}, \quad s = 1, 2, 3, \cdots ,$$

ACKNOWLEDGEMENTS

The author was supported in part by the NSF Undergraduate Research Participation Program in Mathematics at the University of Santa Clara through Grant GY-2645. He also expresses his indebtedness to Prof. Burrowes Hunt for some of the material in the last section.

REFERENCES

1. Garrett Birkoff and Saunders Mac Lane, A Survey of Modern Algebra, MacMillan, New York, 1953.
2. L. Carlitz, "A Note on Fibonacci Numbers," Fibonacci Quarterly, Vol. 2, 1964, pp. 15-28.
3. G. H. Hardy and E. M. Wright, 'An Introduction to the Theory of Numbers, Oxford University Press, London, 1954
4. C. T. Long and J. H. Jordan, "A Limited Arithmetic on Simple Continued Fractions," Fibonacci Quarterly, Vol. 5, 1967, pp. 113-128.

* * * * *

EDITORIAL COMMENT

This special issue is entirely supported by page-charges.