CARLITZ FOUR-TUPLES

MORRIS JACK DeLEON
Florida Atlantic University, Boca Raton, FL 33431-0991

(Submitted August 1986)

Definition 1: We say that $\langle a, b, c, d\rangle$ is a *Carlitz four-tuple* iff a, b, c, d are integers such that $ab \equiv 1 \pmod{c}$, $ab \equiv 1 \pmod{d}$, $cd \equiv 1 \pmod{a}$, and $cd \equiv 1 \pmod{b}$. For convenience, we shall often write CFT instead of Carlitz four-tuple.

As can easily be verified, $\langle 1, 6, 1, 1\rangle$, $\langle 4, 24, 5, 5\rangle$, and $\langle 15, 90, 19, 19\rangle$ are Carlitz four-tuples. More generally, for every integer a, $\langle 1, a, 1, 1\rangle$, $\langle a, a(a+2), a+1, a+1\rangle$, and $\langle a(a+2), a(a+2)(a+3), a(a+3)+1, a(a+3)+1\rangle$ are CFTs. The latter two of these are, in some sense (see the comments between Theorem 17 and Proposition 18), generated by $\langle 1, a, 1, 1\rangle$ and, in fact, $\langle 1, a, 1, 1\rangle$ generates not just these two CFTs but infinitely many CFTs.

Both $\langle 4, 16, 7, 7\rangle$ and $\langle 5, 20, 11, 11\rangle$ are CFTs; more generally, for every integer a, $\langle a, 4a, 2a-1, 2a-1\rangle$ is a CFT.

Carlitz proved in [1] that, if $\langle a, b, c, d\rangle$ is a Carlitz four-tuple, then either $a = b$ or $c = d$. Thus, in the sequel, we shall only consider CFTs of the form $\langle a, b, c, c\rangle$.

There are CFTs $\langle a, b, c, c\rangle$ for which $a = b$ and for which $a = -b$. Some examples are:

$$\langle a, a, a+1, a+1\rangle;\ \langle a, a, a^2-1, a^2-1\rangle;\ \langle a, -a, a^2+1, a^2+1\rangle.$$

Notice also that, if $\langle a, b, c, c\rangle$ is a CFT, then so are $\langle b, a, c, c\rangle$, $\langle -a, -b, c, c\rangle$, $\langle a, b, -c, -c\rangle$, and $\langle -a, -b, -c, -c\rangle$.

Definition 2: The Carlitz four-tuple $\langle a, b, c, c\rangle$ is *primitive* iff there does not exist an integer $m > 1$ such that $\left\langle \frac{a}{m}, bm, c, c\right\rangle$ is a CFT.

The CFTs $\langle 8, 12, 5, 5\rangle$ and $\langle 30, 45, 19, 19\rangle$ are not primitive; for each of these we could choose $m = 2$.

The following result shows that CFTs occur in pairs.

Proposition 3: If $\langle a, b, c, c\rangle$ is a Carlitz four-tuple, then so is

$$\left\langle a, b, \frac{ab-1}{c}, \frac{ab-1}{c}\right\rangle.$$

Proof: Let $d = \frac{ab - 1}{c}$, which is an integer, since $ab \equiv 1 \pmod{c}$. Since $cd = ab - 1 \equiv -1 \pmod{[a, b]}$,

$$1 \equiv c^2d^2 \equiv d^2 \pmod{[a, b]}.$$

Since we also have that $ab = cd + 1 \equiv 1 \pmod{d}$, we see that

$$\left\langle a,\ b,\ \frac{ab - 1}{c},\ \frac{ab - 1}{c} \right\rangle$$

is also a CFT. ■

Given a Carlitz four-tuple $\langle a, b, c, c\rangle$, we shall prove, after a lemma, a necessary and sufficient condition for this CFT to be primitive. Then, after another lemma, we shall prove that $a|b$ for any primitive CFT $\langle a, b, c, c\rangle$.

Lemma 4: Let $\langle a, b, c, c\rangle$ be a Carlitz four-tuple and let m be an integer. We have that $\left\langle \frac{a}{m}, bm, c, c\right\rangle$ is a Carlitz four-tuple iff m divides $\left(a, \frac{c^2 - 1}{b}\right)$.

Proof: First, assume that $\left\langle \frac{a}{m}, bm, c, c\right\rangle$ is a CFT. Thus, $m|a$ and $c^2 \equiv 1 \pmod{bm}$. Since $m|a$ and m divides $\frac{c^2 - 1}{b}$, m divides $\left(a, \frac{c^2 - 1}{b}\right)$.

Conversely, assume that m divides $\left(a, \frac{c^2 - 1}{b}\right)$. Thus, $\frac{a}{m}$ is an integer. Now, since $\langle a, b, c, c\rangle$ is a CFT,

$$\frac{a}{m}bm = ab \equiv 1 \pmod{c}$$

and $c^2 \equiv 1 \pmod{a}$. Hence, $c^2 \equiv 1 \left(\bmod \frac{a}{m}\right)$. Also, since m divides $\frac{c^2 - 1}{b}$, $c^2 \equiv 1 \pmod{bm}$. Therefore, $\left\langle \frac{a}{m}, bm, c, c\right\rangle$ is a CFT. ■

Following directly from Lemma 4 is

Theorem 5: Let $\langle a, b, c, c\rangle$ be a Carlitz four-tuple. We have that $\langle a, b, c, c\rangle$ is a primitive Carlitz four-tuple iff $\left(a, \frac{c^2 - 1}{b}\right) = 1$.

Lemma 6: If $\langle a, b, c, c\rangle$ is a Carlitz four-tuple, then a divides $b\left(a, \frac{c^2 - 1}{b}\right)$.

Proof: Let $e = \frac{c^2 - 1}{b}$. Since a divides $c^2 - 1 = be$ and a divides ab, a divides $(ab, be) = |b|(a, e)$. ■

Proposition 7: If $\langle a, b, c, c\rangle$ is a primitive Carlitz four-tuple, then $a|b$.

Proof: By Lemma 6 and Theorem 5, a divides $b\left(a, \frac{c^2 - 1}{b}\right) = b$. ■

The converse of Proposition 7 is not true. A counterexample is

$$\langle 12, 24, 7, 7\rangle,$$

which is a nonprimitive CFT.

We shall now prove two propositions. Given a CFT, the first proposition will enable us to find the primitive CFT that, in some sense, generates the given CFT. The second proposition does the opposite, i.e., given a primitive CFT, this proposition will enable us to find all CFTs that are generated by the given primitive CFT.

Proposition 8: If $\langle a, b, c, c\rangle$ is a Carlitz four-tuple and $e = \dfrac{c^2 - 1}{b}$, then

$$\left\langle \frac{a}{(a, e)}, b(a, e), c, c\right\rangle$$

is a primitive Carlitz four-tuple.

Proof: By Lemma 4, $\left\langle \dfrac{a}{(a, e)}, b(a, e), c, c\right\rangle$ is a CFT. Since

$$\left(\frac{a}{(a, e)}, \frac{c^2 - 1}{b(a, e)}\right) = \left(\frac{a}{(a, e)}, \frac{e}{(a, e)}\right) = 1,$$

by Theorem 5, $\left\langle \dfrac{a}{(a, e)}, b(a, e), c, c\right\rangle$ is a primitive CFT. ∎

The converse of this result is false. For example, choose $a = 75$, $b = 18$, and $c = 19$. Thus, $e = \dfrac{c^2 - 1}{b} = 20$ and $(a, e) = 5$. Now,

$$\left\langle \frac{a}{(a, e)}, b(a, e), c, c\right\rangle = \langle 15, 90, 19, 19\rangle$$

is a primitive CFT but $\langle a, b, c, c\rangle = \langle 75, 18, 19, 19\rangle$ is not a CFT.

Proposition 9: Let $\langle a, b, c, c\rangle$ be a primitive Carlitz four-tuple. We have that $\left\langle aj, \dfrac{b}{j}, c, c\right\rangle$ is a Carlitz four-tuple iff $j \,\Big|\, \dfrac{b}{a}$.

Proof: First, assume that $\left\langle aj, \dfrac{b}{j}, c, c\right\rangle$ is a CFT. By Lemma 6, Theorem 5, and without loss of generality, assuming $j > 0$, we see that aj divides

$$\frac{b}{j}\left(aj, \frac{c^2 - 1}{b/j}\right) = \frac{b}{j}\left(aj, \frac{j(c^2 - 1)}{b}\right) = b\left(a, \frac{c^2 - 1}{b}\right) = b.$$

Conversely, assume that $aj \mid b$. First, notice that

$$aj\frac{b}{j} = ab \equiv 1 \pmod{c}.$$

Since we have that $c^2 \equiv 1 \pmod{b}$, $aj \mid b$, and $\dfrac{b}{j} \,\Big|\, b$,

$$c^2 \equiv 1 \pmod{aj} \quad \text{and} \quad c^2 \equiv 1 \left(\bmod\ \frac{b}{j}\right). \ ∎$$

The next two theorems (Theorems 10 and 13) consider the cojnection between a CFT $\langle a, b, c, c\rangle$ and the equation $ab + c^2 - 1 = bck$.

Theorem 10: Let a, b, c be integers. We have that $\langle a, b, c, c\rangle$ is a Carlitz four-tuple iff there is an integer k such that $a \mid bk$ and $ab + c^2 - 1 = bck$.

Proof: First, assume that $\langle a, b, c, c\rangle$ is a CFT. Thus, b divides $ab + c^2 - 1$ and c divides $ab + c^2 - 1$. Hence, since $(b, c) = 1$, there is an integer k such that $ab + c^2 - 1 = bck$. Furthermore, since a divides $ab + c^2 - 1 = bck$ and $(a, c) = 1$, a divides bk.

Conversely, assume that there is an integer k such that $a|bk$ and $ab + c^2 - 1 = bck$. Clearly, $ab \equiv 1 \pmod{c}$ and $c^2 \equiv 1 \pmod{b}$. Also, since a divides $bck - ab = c^2 - 1$, $c^2 \equiv 1 \pmod{a}$.

The condition $a|bk$ in Theorem 10 cannot be deleted. For example, let $a = 5$, $b = 8$, $c = 3$, and $k = 2$. Now

$$ab + c^2 - 1 = 48 = bck,$$

but $\langle a, b, c, c\rangle = \langle 5, 8, 3, 3\rangle$ is not a CFT. ∎

Lemma 11: If a, b, c, and k are integers such that $ab + c^2 - 1 = bck$, then $\left(a, \frac{c^2 - 1}{b}\right)$ divides k.

Proof: Let $d = \left(a, \frac{c^2 - 1}{b}\right)$. Since d divides $a + \frac{c^2 - 1}{b} = ck$ and $(d, c) = 1$, d divides k. ∎

Proposition 12: Let a, b, c, and k be integers. If $k|a$, $a|bk$, and $ab + c^2 - 1 = bck$, then $\left\langle\frac{a}{k}, bk, c, c\right\rangle$ is a primitive Carlitz four-tuple and

$$|k| = \left(a, \frac{c^2 - 1}{b}\right).$$

Proof: By Theorem 10, $\langle a, b, c, c\rangle$ is a CFT. Since k divides both a and $ck - a = \frac{c^2 - 1}{b}$, k divides $\left(a, \frac{c^2 - 1}{b}\right)$. This implies, by Lemma 11, that

$$|k| = \left(a, \frac{c^2 - 1}{b}\right).$$

By Proposition 8, $\left\langle\frac{a}{|k|}, b|k|, c, c\right\rangle$ is a primitive CFT. Hence, $\left\langle\frac{a}{k}, bk, c, c\right\rangle$ is a primitive CFT. ∎

The converse of this result is false. For example, choose $a = 75$, $b = 18$, $c = 19$, and $k = 5$.

As a special case of Proposition 12, we have

Theorem 13: Let a, b, c be integers. If $a|b$ and $ab + c^2 - 1 = bc$, then both $\langle a, b, c, c\rangle$ and $\langle a, b, b - c, b - c\rangle$ are primitive Carlitz four-tuples, and if $a|b$ and $ab + c^2 - 1 = -bc$, then both $\langle a, b, c, c\rangle$ and $\langle a, b, b + c, b + c\rangle$ are primitive Carlitz four-tuples.

Proof: We shall just prove this result for $ab + c^2 - 1 = -bc$; the proof for $ab + c^2 - 1 = bc$ is similar. Since $ab + c^2 - 1 = -bc$ and

$$ab + (b + c)^2 - 1 = ab + c^2 - 1 + b^2 + 2bc = b(b + c),$$

by Proposition 12, $\langle -a, -b, c, c\rangle$ and $\langle a, b, b+c, b+c\rangle$ are primitive CFTs. Since $\langle -a, -b, c, c\rangle$ is a primitive CFT, so is $\langle a, b, c, c\rangle$. ∎

The condition $a|b$ cannot be deleted in Theorem 13. For example, for $a = 7$, $b = 30$, and $c = 11$, we see that

$$ab + c^2 - 1 = 330 = bc,$$

but $\langle a, b, c, c\rangle = \langle 7, 30, 11, 11\rangle$ is not even a CFT.

Corollary 14: If a and b are integers greater than 1 such that $a|b$ and $b^2 - 4ab + 4$ is a perfect square, then there is an integer c such that $\langle a, b, c, c\rangle$ is a primitive Carlitz four-tuple and $1 < c < \frac{b}{2}$.

Proof: If we let $c = \frac{b - \sqrt{b^2 - 4ab + 4}}{2}$, then it can easily be shown that $ab + c^2 - 1 = bc$. Therefore, by Theorem 13, $\langle a, b, c, c\rangle$ is a primitive CFT. Also $1 < c < \frac{b}{2}$. ∎

In the preceding corollary, we do need $a|b$; this is shown by considering $a = 7$ and $b = 30$. For assume there is an integer c such that $\langle a, b, c, c\rangle$ is a CFT. Thus, by Theorem 10, there is an integer k such that

$$7(30) + c^2 - 1 = 30ck.$$

This implies that $c|209$, so $c = 11$ or $c = 19$. Neither of these is possible, since we must have $c^2 \equiv 1 \pmod 7$.

Using the following lemma, we shall find a connection between a diophantine equation and primitive CFTs.

Lemma 15: For a, b, c, q complex numbers with $q = b/a$, we have that

$$ab + c^2 - 1 = bc$$

iff

$$(b - 2c)^2 - (q^2 - 4q)a^2 = 4.$$

Proof: Since $b = aq$, this result follows from the identity

$$\begin{aligned}(b - 2c)^2 - (q^2 - 4q)a^2 &= b^2 - 4bc + 4c^2 - (qa)^2 + 4a(qa)\\ &= b^2 - 4bc + 4c^2 - b^2 + 4ab = 4(ab + c^2 - bc).\end{aligned}$$

Theorem 16: If q, u, v are integers such that $u^2 - (q^2 - 4q)v^2 = 4$, then both

$$\left\langle v, qv, \frac{qv-u}{2}, \frac{qv-u}{2}\right\rangle \quad \text{and} \quad \left\langle v, qv, \frac{qv+u}{2}, \frac{qv+u}{2}\right\rangle$$

are primitive Carlitz four-tuples.

Proof: Let $a = v$, $b = qv$, and $c = \frac{qv - u}{2}$. Thus, $a|b$ and

$$(b - 2c)^2 - (q^2 - 4q)a^2 = u^2 - (q^2 - 4q)v^2 = 4.$$

Therefore, by Lemma 15 and Theorem 13, the proof is complete. ■

As we saw in the preceding theorem, there is a strong connection between primitive CFTs and the diophantine equation

$$u^2 - (q^2 - 4q)v^2 = 4.$$

For this reason, we shall now consider the diophantine equation

$$u^2 - Dv^2 = 4, \tag{1}$$

where D is a natural number that is not a perfect square. Our discussion will be based on work by Trygve Nagell [2, pp. 3-4].

If $u = u^*$ and $v = v^*$ are integers which satisfy (1), then we say, for simplicity, that the number $u^* + v^*\sqrt{D}$ is a solution of (1). From among all solutions in positive integers to (1), there is a solution in whch both u and v have their least positive values; this solution is called the *fundamental solution of* (1). The following theorem [2, Theorem 1] states that from the fundamental solution of (1), one can generate all solutions in positive integers to (1).

Theorem 17: We have that $u + v\sqrt{D}$ is a solution in positive integers to (1) iff there is a positive integer n such that

$$\frac{1}{2}(u + v\sqrt{D}) = \left[\frac{1}{2}(u_1 + v_1\ D)\right]^n,$$

where $u_1 + v_1\sqrt{D}$ is the fundamental solution to (1).

For $D = a^2 - 4a$, we can easily see that $(a - 2) + \sqrt{D}$ is a fundamental solution to (1). Thus, by Theorem 16, $\langle 1, a, 1, 1\rangle$ is a primitive CFT. In some sense, from a trivial solution to (1), we obtained a trivial CFT. It turns out though that from this trivial fundamental solution to (1), we can get some distinctly nontrivial primitive CFTs.

Using Theorem 17 and doing some calculations, we see that two more solutions to (1) are

$$u_2 + v_2\sqrt{D} = (a^2 - 4a + 2) + (a - 2)\sqrt{D}$$

and

$$u_3 + v_3\sqrt{D} = (a - 2)(a^2 - 4a + 1) + (a - 3)(a - 1)\sqrt{D},$$

where $D = a^2 - 4a$. Using Theorem 16 and, for convenience, replacing a by $a + 2$, we see that $u_2 + v_2\sqrt{D}$ gives rise to

$$\langle a, a(a+2), a+1, a+1\rangle \text{ and } \langle a, a(a+2), a^2+a-1, a^2+a-1\rangle,$$

and $u_3 + v_3\sqrt{D}$, with a replaced by $a + 3$, gives rise to

$$\langle a(a+2), a(a+2)(a+3), a(a+3)+1, a(a+3)+1\rangle$$

and

$$\langle a(a+2), a(a+2)(a+3), a(a+1)(a+3)-1, a(a+1)(a+3)-1\rangle.$$

Of course, using Theorems 17 and 16, we could continue to get infinitely many primitive CFTs from the fundamental solution $(a - 2) + \sqrt{D}$, where $D = a^2 - 4a$.

Notice also that, for any integer a, $u = 2$ and $v = a$ is a solution to (1), where $D = 4^2 - 4 \cdot 4 = 0$. This gives rise to the primitive CFTs

$$\langle a, 4a, 2a-1, 2a-1\rangle \text{ and } \langle a, 4a, 2a+1, 2a+1\rangle.$$

The preceding discussions gives

Proposition 18: For all integers a, the following are primitive CFTs:

$$\langle 1, a, 1, 1\rangle \text{ and } \langle 1, a, a-1, a-1\rangle;$$
$$\langle a, 4a, 2a-1, 2a-1\rangle \text{ and } \langle a, 4a, 2a+1, 2a+1\rangle;$$
$$\langle a, a(a+2), a+1, a+1\rangle \text{ and } \langle a, a(a+2), a^2+a-1, a^2+a-1\rangle;$$
$$\langle a(a+2), a(a+2)(a+3), a(a+3)+1, a(a+3)+1\rangle \text{ and}$$
$$\langle a(a+2), a(a+2)(a+3), a(a+1)(a+3)-1, a(a+1)(a+3)-1\rangle.$$

The next result relates CFTs to another diophantine equation.

Proposition 19: For a, b, c integers, we have that $ab + c^2 - 1 = bc$ iff

$$a^2 + c^2 + (b-c)^2 - (b-a)^2 = 2.$$

Proof: This result follows from the identity

$$\begin{aligned} &a^2 + c^2 + (b-c)^2 - (b-a)^2 \\ &= a^2 + c^2 + b^2 - 2bc + c^2 - b^2 + 2ab - a^2 \\ &= 2ab + 2c^2 - 2bc = 2(ab + c^2 - bc). \ \blacksquare \end{aligned}$$

The following two results concern the relative size of a, b, and c, where $\langle a, b, c, c\rangle$ is a Carlitz four-tuple.

Lemma 20: Let $\langle a, b, c, c\rangle$ be a Carlitz four-tuple. If $0 < a < c < b$, then $ab + c^2 - 1 = bc$.

Proof: Since $0 < a < c < b$,

$$0 < ab + c^2 - 1 < bc + bc - 1 < 2bc.$$

Furthermore, by Theorem 10, $ab + c^2 - 1 = bc$. $\blacksquare$

Theorem 21: Let $\langle a, b, c, c\rangle$ be a Carlitz four-tuple. If $0 < a < c < b$, then $\langle a, b, c, c\rangle$ is a primitive Carlitz four-tuple.

Proof: By the preceding lemma, $ab + c^2 - 1 = bc$. Thus,

$$\left(a, \frac{c^2 - 1}{b}\right) = (a, c - a) = (a, c) = 1.$$

Thus, by Theorem 5, $\langle a, b, c, c\rangle$ is a primitive Carlitz four-tuple. ∎

Theorem 22: Let a, b, and c be positive integers such that $a \neq b$, $c > 1$, and $c \neq ab - 1$. The following six conditions are equivalent.

(i) If, for some integer k, $ab + c^2 - 1 = bck$ and a divides $c^2 - 1$, then $k|a$.

(ii) If $\langle a, b, c, c\rangle$ is a Carlitz four-tuple, then $ab + c^2 - 1 = bc(a, e)$, where $e = \dfrac{c^2 - 1}{b}$.

(iii) If $\langle a, b, c, c\rangle$ is a primitive Carlitz four-tuple, then

$$ab + c^2 - 1 = bc.$$

(iv) If $\langle a, b, c, c\rangle$ is a primitive Carlitz four-tuple, then

$$u^2 - (q^2 - 4q)v^2 = 4,$$

where $u = b - 2c$, $v = a$, and $q = b/a$.

(v) If $\langle a, b, c, c\rangle$ is a primitive Carlitz four-tuple, then

$$0 < a < c < b.$$

(vi) If $\langle a, b, c, c\rangle$ is a primitive Carlitz four-tuple, then

$$b^2 - 4ab + 4 = (b - 2c)^2.$$

We see that statements (ii)-(vi) in Theorem 22 are related to Theorem 10 and also to the converses of Theorems 13, 16, and 21, and Corollary 14, respectively.

Proof: First, we show that (i), (ii), and (iii) are equivalent. We then show that (iii) is equivalent to each of (iv), (v), and (vi).

Proof that (i) implies (iii): Assume that $\langle a, b, c, c\rangle$ is a primitive CFT. Thus, by Theorem 10, for some integer k, $ab + c^2 - 1 = bck$. Hence, by (i), we have $k|a$. Thus, k divides $ck - a = \dfrac{c^2 - 1}{b}$. Hence, k divides $\left(a, \dfrac{c^2 - 1}{b}\right) = 1$ by Theorem 5. Therefore, $ab + c^2 - 1 = bck = bc$.

Proof that (iii) implies (ii): Assume that $\langle a, b, c, c\rangle$ is a Carlitz four-tuple. By Proposition 8, $\left\langle \dfrac{a}{(a, e)}, b(a, e), c, c\right\rangle$ is a primitive CFT. Thus, by (iii), $ab + c^2 - 1 = bc(a, e)$.

Proof that (ii) implies (i): Assume that a divides $c^2 - 1$ and, for some integer k, $ab + c^2 - 1 = bck$. Since $a|bck$ and $(a, c) = 1$, $a|bk$. Thus, by

Theorem 10, $\langle a, b, c, c \rangle$ is a CFT. Hence, by (ii), $ab + c^2 - 1 = bc(a, e)$. Therefore, $k = (a, e)$, so $k|a$.

Proof that (iii) and (iv) are equivalent: This follows from Lemma 15.

Proof that (iii) implies (v): Assume that $\langle a, b, c, c \rangle$ is a primitive CFT. Thus, $ab + c^2 - 1 = bc$.

First, assume $c \geqslant b$. Since $c^2 \geqslant bc = ab + c^2 - 1$, we have the contradiction that $1 \geqslant ab$.

Second, assume that $a \geqslant c$. Since $ab \geqslant bc = ab + c^2 - 1$, we have the contradiction that $1 \geqslant c^2$.

Proof that (v) implies (iii): This follows from Lemma 20.

Proof that (iii) and (vi) are equivalent: This follows from the identity

$$(b - 2c)^2 - b^2 + 4ab = 4(ab + c^2 - bc). \blacksquare$$

Based on some computer-genreated data, it seems reasonable to believe that Theorem 22(iii) is true. Hence, we make the following conjecture.

Conjecture 23: The six statements of Theorem 22 are true.

REFERENCES

1. L. Carlitz. "An Application of the Reciprocity Theorem for Dedekind Sums." *The Fibonacci Quarterly* 22 (1984):266-270.
2. Trygve Nagell. "Contributions to the Theory of a Category of Diophantine Equations of the Second Degree with Two Unknowns." *Nova Acta Soc. Sci. Upsal.* (4) **16**, no. 2 (1955), 38 pp.

◆◇◆◇◆