RECURSIONS FOR CARLITZ TRIPLES

Paul Duvall and Theresa P. Vaughan

University of North Carolina at Greensboro, Greensboro, NC 27412

(Submitted March 1987)

1. Introduction

In [1], using the properties of the reciprocity law for Dedekind sums, L. Carlitz proved that the system

$$\begin{aligned} hh' &\equiv 1 \pmod{k}, \quad hh' \equiv 1 \pmod{k'} \\ kk' &\equiv 1 \pmod{h}, \quad kk' \equiv 1 \pmod{h'} \end{aligned} \tag{*}$$

has no positive integral solutions unless either $k = k'$ or $h = h'$.

In [2], M. DeLeon studied (essentially) solutions of the system (*). He defines a Carlitz four-tuple (a, b, c, c) by: a, b, c are integers (not required to be positive), $ab \equiv 1 \pmod{c}$, $c^2 \equiv 1 \pmod{a}$, and $c^2 \equiv 1 \pmod{b}$. He introduces the notion of a primitive Carlitz four-tuple (a, b, c, c), that is, one with the property that there exists no integer $m > 1$ such that one also has that $(a/m, bm, c, c)$ is a Carlitz four-tuple. We mention here two of his results, which are basic to our work in this paper: the Carlitz four-tuple (a, b, c, c) is primitive if and only if the greatest common divisor

$$\gcd(a, (c^2 - 1)/b) = 1,$$

and secondly, if (a, b, c, c) is primitive, then a divides b.

In this paper we consider only the positive integral solutions of the system (*). Since at most three different integers are involved, we use the notation (a, b, c) for a solution, with $ab \equiv 1 \pmod{c}$, $c^2 \equiv 1 \pmod{a}$, and $c^2 \equiv 1 \pmod{b}$; we call this a Carlitz triple (CT). The results of [2] of course apply to these triples. A primitive CT will be called a PCT.

In Section 2, we first prove some elementary arithmetic properties of a PCT, and then prove the following conjecture from [2]:

If (a, b, c) is a PCT with $a \neq b$, $c > 1$, $c \neq ab - 1$,
then we have: $0 < a < c < b$.

In Section 3, we show that the set of all PCT's (a, ax, c) with $c > 2$, and for a fixed integer $x > 3$, satisfy a recursive relation. The original recursions (resulting directly from a study of these PCT's) are not very pretty, but they reduce to a surprisingly simple form.

In Section 4, we give the generating functions associated with the recurrences from Section 3; these are rational functions whose denominator is quadratic.

The reader will notice that many of our results are stated with assorted minor restrictions (e.g., $c > 1$, or $a < b$, and so on). In Section 5, we discuss the reasons for such restrictions. It is then seen that only one interesting case [out of all possible positive solutions to the system (*)] is not covered. This is the case of those PCT's of the form (a, a, c), to which, of course, the conjecture of DeLeon does not apply. We hope to say more about these in a later paper.

2. Elementary Properties

In this section we first develop some of the arithmetic consequences of the definition of a PCT (a, b, c). Recall that a CT is a triple of positive integers a, b, c satisfying:

$$a \le b$$

$$ab \equiv 1 \pmod{c}$$
$$c^2 \equiv 1 \pmod{a}$$
$$c^2 \equiv 1 \pmod{b}.$$

The PCT triples also satisfy the additional conditions

$$a \mid b$$

$$\gcd(a, (c^2 - 1)/b) = 1.$$

Lemma 2.1: Let (a, b, c) be a PCT with $c > 1$.

Then there exist integers x, r, u so that $x > 0$, $u > 0$, $r \ge 0$, and

(i) $b = ax$

(ii) $c^2 - 1 = ax(uc - a)$, $(a, u) = (a, uc - a) = 1$

(iii) $a^2x = 1 + rc$.

Proof: Since $a \mid b$, (i) is true for some $x > 0$. Then $ab = a^2x$ and (iii) follows since $ab \equiv 1 \pmod{c}$. We know that $b = ax$ divides $c^2 - 1$, that is, $c^2 - 1 = axt$ for some integer t; $t > 0$ since $c > 1$. Since $axt \equiv -1 \pmod{c}$ and $a^2x \equiv 1 \pmod{c}$, then $t \equiv -a \pmod{c}$. We claim that $t = uc - a$ with u a positive integer. If $c = 2$, this is seen directly: $c^2 - 1 = 3 = axt$ implies that a, x, and t can only take on the values 1 or 3. If $a = x = 1$, then $u = 2$; if $a = 3$, $x = 1$, $t = 1$, then $u = 2$; if $a = 1$, $x = 3$, $t = 1$, then $u = 1$. If $c > 2$, then since $t \equiv -a \pmod{c}$ and t, a, and c are all positive, then $t = uc - a$ for some $u > 0$. Note that r can be 0 if and only if $a = b = x = 1$; otherwise $r > 0$. □

Corollary 2.1: Let (a, b, c) be a PCT with $c > 1$, and suppose the integers x, r, u are given as in Lemma 2.1. Then $(uc - a, x(uc - a), c)$ is also a PCT with $c > 1$. □

Remark: Later on, for a given $x > 3$, we will be considering the set of all PCT's (a, b, c) for which $b/a = x$. It will be useful to note that, if (a, ax, c) is a PCT with $c > 2$, then one of the two PCT's (a, ax, c) and $(uc - a, x(uc - a), c)$ has its left-most member less than c. [This follows from Lemma 2.1(ii); $a(uc - a)$ divides $c^2 - 1$, so one of the factors must be less than c.]

Lemma 2.2: Let (a, b, c) be a PCT with $c > 1$, and suppose the integers x, r, u are given as in Lemma 2.1. Then

(i) $c = axu - r$

(ii) $(ru - a)c = ar - u$

(iii) $(a^2 - u^2)(r^2 - 1) = (c^2 - 1)(ru - a)^2$.

Proof: From the proof of Lemma 2.1, we have $x = b/a$, $r = (ab - 1)/c$, and $u = (c^2 - 1 + ab)/bc$. The result follows easily from these equalities. □

Theorem 2.1: Let (a, b, c) be a PCT with $a > 1$ and $c > 1$, and suppose the integers x, r, u are given as in Lemma 2.1. Then $r > 1$, and (a, b, r) is a PCT.

Proof: First, since $a > 1$, then $a^2x = 1 + rc > 1$ [Lemma 2.1(iii)] and so $r > 0$. Now consider Lemma 2.2(ii) with $r = 1$. It reduces to $(u - a)c = a - u$. We have $c > 0$, so this implies $a = u$. But $(a, u) = 1$ by Lemma 2.1(ii), and so $u = 1$ and $a = 1$, contradicting the assumption that $a > 1$; thus $r > 1$. Next, since $a^2x = 1 + rc$ and $c = axu - r$, then

$$a^2x = 1 + r(axu - r) = 1 + (uax)r - r^2$$

$$ax(a - ur) = 1 - r^2$$

and so $r^2 \equiv 1 \pmod{a}$ and $r^2 \equiv 1 \pmod{b}$ (since $b = ax$).

From Lemma 2.1(iii) we already have $ab = a^2x \equiv 1 \pmod{r}$. It remains to show that (a, b, r) is primitive, that is (see [2]), that

$$\gcd(a, (r^2 - 1)/ax) = \gcd(a, ru - a) = 1.$$

From Lemma 2.1(ii) and the fact that (a, b, c) is primitive, we have

$$\gcd(a, u) = 1.$$

Lemma 2.1(iii) implies that

$$\gcd(a, r) = 1.$$

Then $\gcd(a, ru - a) = 1$ also. □

The following theorem settles the conjecture of DeLeon in the affirmative.

Theorem 2.2: Let (a, b, c) be a PCT with $0 < a < b$ and $c > 1$. If $a < c$, then $b > c$.

Proof: First, if $a = 1$, then we have, by Lemma 2.1(iii), that $a^2x = x = 1 + rc$. Since $b = ax$, and $b > 1$, then $r > 0$ and so $b \geq c + 1$. Thus, the theorem is true for $a = 1$ and $c > 2$. For $a > 1$, the proof is by descent. (We use the notation of Lemma 2.1.) Suppose the contrary, and let c be the smallest positive integer such that there exist integers a, x so that, with $b = ax$, one has that (a, b, c) is a PCT with $a < c$ and $b < c$, $a < b$ and $c > 1$. Note now that, since we have $b > a$, then $x > 1$. Since $ax < c$, then $a^2x < ac$. Then

$$a^2x = 1 + rc < ac,$$

and hence $r < a$. By Theorem 2.1, (a, ax, r) is also a PCT and has $r > 1$, and by Corollary 2.1, $(a', b', c') = (ru - a, x(ru - a), r)$ is a PCT. Since $a > r$, and since $r^2 - 1 = ax(ru - a)$ then $x(ru - a) < r$. Thus,

$$a' < c',\ b' < c',\ a' < b', \text{ and } r > 1.$$

We have $r < a \leq ax < c$, which contradicts the minimality of c. This completes the proof. □

Corollary 2.2: Let (a, b, c) be a PCT with $0 < a < b$, and with $c > 1$, and suppose the integers x, r, u are given as in Lemma 2.1. Assume that $a < c$. Then $u = 1$.

Proof: By Theorem 2.2, $ax > c$, so from Lemma 2.1(ii) it follows that

$$0 < uc - a < c.$$

Since $a < c$, then it must be that $u = 1$. □

3. The Recursion for PCT's

Consider the set $S(t)$ of all PCT's of the form $(a, a(t+1), c)$, where $c > 2$ and $t > 2$. In this section, we show that for each $t > 2$, $S(t)$ is a recursively defined sequence of triples, with initial element $(1, t+1, t)$.

These conditions of course imply that Theorem 2.2 and its Corollary will apply to all these PCT's. In particular, in the notation of Lemma 2.1, for any PCT (a, b, c) in this section we will always have $u = 1$.

Lemma 3.1: Let (a, b, c) be a PCT with $a < b$ and $c > 2$, and r as defined in Lemma 2.1. If $a < c/2$, then $r \le c - 2$; if $a > c/2$, then $r > c$.

Proof: We use the notation of Lemma 2.1. Note that

$$(r+1)(c+1) = rc + 1 + r + c.$$

By Corollary 2.2, $u = 1$ and so, from Lemma 2.2(i), $ax = r + c$.

By Lemma 2.1(iii), $a^2x = rc + 1$. Hence, we have

$$(r+1)(c+1) = a^2x + ax = ax(a+1).$$

If $a < c/2$, then $a + 1 \le c - a$. Then,

$$(r+1)(c+1) \le ax(c-a) = c^2 - 1,$$

which implies that $r \le c - 2$; similarly, if $c/2 < a < c$, then $a + 1 > c - a$, and then $r > c - 2$. Note that $a = c/2$ is not possible if c is odd; if c is even and $c > 2$, then $(a, c) = 1$ implies that $a \ne c/2$. [Lemma 2.1(iii) implies that $(a, c) = 1$.] By Lemma 2.2(ii), since $u = 1$, we have

$$(r-a)c = ar - 1,$$

so that $(r, c) = 1$ and hence $r \ne c$. It remains to show that $r \ne (c-1)$. Suppose to the contrary that $r = c - 1$. By Lemma 2.2(i) then, $ax = 2c - 1 > 3$. Since ax must divide $c^2 - 1$, while $\gcd(2c-1, c-1) = 1$, then $2c - 1$ must divide $c + 1$; this is impossible for $c > 2$. Thus, $r \ne c - 1$, and it follows that $r > c$. □

Lemma 3.2: Suppose that (a, ax, r) and (a, ax, k) are both PCT's with $r, k > 2$ and $x > 3$, and that $r \ne k$. Then $a^2x = 1 + rk$, and $r + k = ax$.

Proof: By Corollary 2.2, $u = 1$. Then, from Lemmas 2.1 and 2.2, we must have:

$$\begin{aligned}
&r^2 - 1 = ax(r-a)\\
&a^2x = 1 + rm \text{ (for some positive integer } m)\\
&r + m = ax\\
&k^2 - 1 = ax(s-a)\\
&a^2x = 1 + kn \text{ (for some positive integer } n)\\
&k + n = ax.
\end{aligned}$$

Then

$$a^2x = 1 + m(ax - m) = 1 + n(ax - n),$$

and then

$$(m-n)ax = m^2 - n^2,$$

which gives $ax = m + n$. Then $k = m$ and $r = n$. □

Lemma 3.3: If (a, ax, c) is a PCT with $c > 2$ and $x > 3$, and if $a^2x = 1 + rc$, then $r \ne c$.

Proof: If $r = 1$, clearly $r \neq c$. Suppose $r > 1$. Since $a^2x = 1 + rc$ implies that $(a, r) = 1$ and $r > 1$, then $r \neq a$. By Lemma 2.2 and Corollary 2.2,

$$(r - a)c = ra - 1.$$

Thus, r and c must be relatively prime. Since $c > 1$, then $r \neq c$. □

Corollary 3.3: Suppose that (a, ax, c) is a PCT with $c > 2$ and $x > 3$, and with $a^2x = 1 + rc$ and $a > c/2$. Then the PCT (a, ax, r) has $r > c$ and $a < r/2$.

Proof: For the PCT (a, b, c), Lemma 3.1 says that $r > c$. Applying Lemma 3.1 to the PCT (a, b, r) completes the proof. □

Remark: Observe that, given any PCT (a, b, c) with $b/a = x > 3$ and $c > 2$, there are two more PCT's particularly associated with it, in which the quotient of the second element by the first is also x, namely

$$(c - a, (c - a)x, c) \quad \text{and} \quad (a, b, r).$$

By Lemmas 3.1 and 3.2, there are exactly two such triples, and, in the lexicographic ordering of all triples, one of these associated triples is "less than" (a, b, c), and the other one is "greater."

Example: $x = 5$; $c_0 = 4 = x - 1$; $a = 1$. Then $(1, 5, 4)$ is a PCT;

$$a^2x = 5 = 1 + 4.$$

Also $(3, 15, 4)$ is a PCT so we have $a = 3$ and

$$a^2x = 45 = 1 + 4 \times 11.$$

[Note that $3 = c_0 - 1$, and $11 = c_0^2 - c_0 - 1 = c_1$.]

Now $(3, 15, 11)$ is a PCT (Theorem 2.1). Wishing still to go up, use the related PCT $(8, 40, 11)$ (Corollary 2.1); then $a = 8$ and we have

$$a^2x = 1 + 11 \times 29.$$

Put $c_2 = 29$.

[Note that $8 = 11 - 3 = (c_1 - c_0 + 1)$.]

We now have that $(8, 40, 29)$ and $(21, 5 \times 21, 29)$ are PCT's. With $a = 21$, then

$$a^2x = 1 + 29 \times 76.$$

Put $c_3 = 76$.

[Note that $21 = c_2 - c_1 + c_0 - 1$.]

For convenience, we state this rather commonplace observation as a theorem.

Theorem 3.1: The set $S(t)$ of all PCT's $(a, a(t + 1), c)$ with $a > 0$, $c > 2$, $t > 2$, is linearly ordered by the lexicographic order:

$$A_0, A_1, A_2, \ldots,$$

where $A_0 = (1, t + 1, t)$, and if $A_n = (a, a(t + 1), c)$ with $a < c/2$, then

$$A_{n+1} = (c - a, (c - a)(t + 1), c);$$

if $A_n = (a, a(t + 1), c)$ with $a > c/2$, then

$$A_{n+1} = (a, a(t + 1), (a^2(t + 1) - 1)/c). \ \square$$

The first few members of $\{A_i\}$ are:

$$A_0 = (1,\ t + 1,\ t)$$
$$A_1 = (t - 1,\ (t - 1)(t + 1),\ t)$$
$$A_2 = (t - 1,\ (t - 1)(t + 1),\ t^2 - t - 1)$$
$$A_3 = (t^2 - 2t,\ (t^2 - 2t)(t + 1),\ t^2 - t - 1).$$

Let $(x_0, x_1, x_2, \ldots)$ be the sequence of the left-hand entries of the A_i, and define a sequence (a_n) as follows:

$$a_0 = 1,\ a_1 = t - 1,$$

and then, for all $i > 1$, $a_i = x_{2i-1}$. That is, (a_n) is the sequence of the distinct left-hand entries of the triples A_i. We proceed similarly on the right; it will be convenient to furnish this sequence with an "extra" initial term:

$$c_0 = 1,\ c_1 = t,\ c_2 = t^2 - t - 1,\ \ldots .$$

From the definition, we have that

$$a_n = c_n - a_{n-1} \quad \text{and} \quad c_{n+1} = (a_n^2 (t + 1) - 1)/c_n.$$

Theorem 3.2: For fixed t, $t > 2$, the sequences $\{a_n\}$ and $\{c_n\}$ defined above satisfy

(i) $a_n = c_n - c_{n-1} + \cdots + (-1)^j c_{n-j} + \cdots + (-1)^n \quad (n \geq 0)$

(ii) $c_{n+1} = (t + 1)c_n - 2(t + 1)a_{n-1} + c_{n-1} \quad (n \geq 1).$

Proof: Since $a_0 = 1 = (-1)^0$, then (i) follows by induction from the definition of $\{A_i\}$.

We have $c_0 = 1$, and $c_1 = t$, so

$$c_2 = t^2 - t - 1 = (t + 1)c_1 - 2(t + 1)a_0 + c_0.$$

From the definition of $\{A_i\}$, if $n > 2$, we have

$$\begin{aligned} c_n &= \{(t + 1)(c_{n-1} - c_{n-2} + \cdots + (-1)^n)^2 - 1\}/c_{n-1} \\ &= [(t + 1)\ c_{n-1}^2 + 2c_{n-1}(-c_{n-2} + c_{n-3} - \cdots + (-1)^n \\ &\qquad + (-c_{n-2} + c_{n-3} + \cdots + (-1)^n)^2 - 1]/c_{n-1} \\ &= (t + 1)c_{n-1} + 2(t + 1)(-c_{n-2} + c_{n-3} - \cdots + (-1)^n) \\ &\qquad + \{(t + 1)(-c_{n-2} + c_{n-3} - \cdots + (-1)^n)^2 - 1\}/c_{n-1} \\ &= (t + 1)c_{n-1} + 2(t + 1)(-a_{n-1}) + \{(t + 1)(a_{n-2})^2 - 1\}/c_{n-1}. \end{aligned}$$

From the definition of $\{A_i\}$, we know that

$$\{(t + 1)(a_{n-2})^2 - 1\}/c_{n-2} = c_{n-1},$$

and this proves (ii). □

Using this result, one can establish that the sequences $\{a_n\}$ and $\{c_n\}$ do in fact satisfy recursions of a much simpler nature.

Theorem 3.3: For fixed t, $t > 2$, the sequences $\{a_n\}$ and $\{c_n\}$ satisfy, for $n \geq 1$:

(i) $c_{n-1} + c_n = (t + 1)a_{n-1}$

(ii) $a_{n+1} = (t - 1)a_n - a_{n-1}$

(iii) $c_{n+1} = (t - 1)c_n - c_{n-1}.$

Proof: It is easy to verify that (i), (ii), (iii) are all true for $n = 1, 2, 3$. Suppose they are true for all k, $1 \le k \le n$. From Theorem 3.2 and the inductive hypothesis, we have

$$\begin{aligned} c_{n+1} &= (t+1)c_n + 2(t+1)(-a_{n-1}) + c_{n-1} \\ &= (t+1)c_n - 2(c_n + c_{n-1}) + c_{n-1} \\ &= (t-1)c_n - c_{n-1}. \end{aligned}$$

It then follows that

$$\begin{aligned} c_{n+1} + c_n &= tc_n - c_{n-1} = (t+1)c_n - c_n - c_{n-1} \\ &= (t+1)(c_n - a_{n-1}) = (t+1)a_n. \end{aligned}$$

Since $a_n = c_n - a_{n-1}$, statement (ii) follows from (iii); this completes the proof. □

4. Generating Functions

It is well known that recursive sequences like $\{a_n\}$ and $\{c_n\}$ are naturally associated with generating functions, which may be found and described in a standard way. In this section we give the generating functions and the corresponding Binet formulas without proof.

Let t be a fixed integer, $t > 2$, and consider the sequences $\{a_n\}$ and $\{c_n\}$ defined in Section 3. Define two formal power series by

$$F(z) = \sum_{i=0}^{\infty} c_i z^i; \quad G(z) = \sum_{i=0}^{\infty} a_i z^i.$$

Theorem 4.1: The series defined above satisfy

$$F(z) = (1+z)/(1+(1-t)z+z^2); \quad G(z) = F(z)/(1+z). \ \square$$

If $t = 3$, then

$$z^2 + z(1-t) + 1 = (z-1)^2,$$

while, if $t > 3$, then $z^2 + z(1-t) + 1$ has irrational roots. Thus, we consider two cases separately.

Theorem 4.2: If $t = 3$, then

$$F(z) = \sum (i+1)z^i;$$

$a_n = n + 1$ and $c_n = 2n + 1$. □

Theorem 4.3: Let $t > 3$, and let α, β be the two roots of $z^2 + (1+t)z + 1$. Then $\alpha \neq \beta$, and we have

$$a_n = (\alpha^{n+1} - \beta^{n+1})/(\alpha - \beta)$$

and

$$c_n = (\alpha^{n+1} + \alpha_n - \beta^{n+1} - \beta_n)/(\alpha - \beta). \ \square$$

5. Some Exceptions

In this section we discuss the reasons for the restrictive conditions attached to some of our results. Throughout we use the notation of Lemma 2.1; (a, b, c) is a PCT, a, b, c are positive integers, and so on.

A. If $c = 1$: For all positive a, b, $(a, b, 1)$ is a CT and is primitive if and only if $a = 1$.

B. If $c = 2$: The only PCT's with $c = 2$ are (1, 1, 2), (1, 3, 2), and (3, 3, 2).

C. If $c > 2$, there are no PCT's of the form $(a, 2a, c)$ or $(a, 3a, c)$.

D. There are PCT's of the form (a, a, c), for instance (8, 8, 3). However, these seem to differ from those with $a < b$ in various essential ways; in particular, they do not appear to fit into a single recurrence scheme. Note that DeLeon's conjecture does not apply to these PCT's.

Statements (A) and (B) are easily checked. To see (C), suppose first that $(a, 2a, c)$ is a PCT with $c > 2$. Then, by Theorem 2.2, we have $a < c < 2a$; and by Corollary 2.2 and Lemma 2.1, we can write

$$c^2 - 1 = 2a(c - a) = 2ac - 2a^2.$$

Rearranging, we get

$$c^2 - 2ac + a^2 = 1 - a^2$$
$$(c - a)^2 = 1 - a^2.$$

Since $c > a$, this is positive, contradicting the fact that $a > 0$. Therefore, $(a, 2a, c)$ can only be a PCT if $c = 1, 2$.

Proceeding similarly with a PCT of the form $(a, 3a, c)$ with $c > 2$, we get $a < c < 3a$ and

$$c^2 - 1 = 3a(c - a)$$
$$(c - a)^2 = 1 + a(c - 2a).$$

Since $c > a$, this is positive, so $c \geq 2a$. Rearranging the first equation in another way, we get

$$c^2 - 3ac + 2a^2 = 1 - a^2$$
$$(c - a)(c - 2a) = 1 - a^2.$$

Since $c \geq 2a$, we must have $a = 1$. A CT (a, b, c) must satisfy $ab \equiv 1 \pmod{c}$ and $c^2 \equiv 1 \pmod{a, b}$. Here we have $a = 1$, $b = 3$; then $ab \equiv 1 \pmod{c}$ implies $c \leq 2$. Thus, there are no PCT's with $c > 2$ and the form $(a, 3a, c)$.

References

1. L. Carlitz. "An Application of the Reciprocity Theorem for Dedekind Sums." *Fibonacci Quarterly 22* (1984).
2. M. J. DeLeon. "Carlitz Four-Tuples." *Fibonacci Quarterly* (to appear).

*****