

# Daisy chains—a fruitful combinatorial concept

D. A. PREECE

*School of Mathematical Sciences  
Queen Mary, University of London  
Mile End Road, London E1 4NS  
U.K.*

D.A.Preece@qmul.ac.uk

and

*Institute of Mathematics, Statistics and Actuarial Science  
Cornwallis Building, University of Kent  
Canterbury, Kent CT2 7NF  
U.K.*

## Abstract

“*Daisy, Daisy, give me your answer, do!*” [10]

For any positive integer  $n$ , the units of  $\mathbb{Z}_n$  are those elements of  $\mathbb{Z}_n \setminus \{0\}$  that are coprime with  $n$ . The number of units in  $\mathbb{Z}_n$  is given by Euler’s totient function  $\phi(n)$ . If  $n$  is odd, a *daisy chain* for the units of  $\mathbb{Z}_n$  is obtained by arranging the units of  $\mathbb{Z}_n$  on a circle in some order  $[a_1, a_2, \dots, a_{\phi(n)}]$  such that the set of differences  $b_i = a_{i+1} - a_i$  ( $i = 1, 2, \dots, \phi(n)$ , with  $a_{\phi(n)+1} = a_1$ ) is itself the set of units. Various constructions are given for daisy chains for odd values of  $n$  that have the prime-power decompositions  $p^i$  ( $i \geq 1$ ),  $p^i q^j$  ( $i \geq 1, j \geq 1$ ) and  $pqr$  (where  $p, q$  and  $r$  are distinct odd primes). The paper’s emphasis is on values of  $n$  lying in the range  $1 < n < 300$ , within which every prime-power decomposition of an odd value  $n$  is of one of the types just given. The concept of *fertile* daisy chains is defined, and the link between daisy chains and terraces is briefly outlined.

## 1 Introduction

This paper introduces the combinatorial concept of a *daisy chain* for the units of  $\mathbb{Z}_n$  where  $n$  is odd. If  $n$  is an odd prime, a daisy chain for the units of  $\mathbb{Z}_n$  is a *directed R-terrace* for  $\mathbb{Z}_n$  [15, p. 252] and is equivalent to a *total cycle* in the sense of Azais

[4]. (In these circumstances, a daisy chain provides a partition of the edges of  $2K_n$  into cycles of length  $n - 1$ , invariant under a group acting regularly.) However, for odd values of  $n$  that are not prime the concept of a daisy chain seems to be new. Although this new approach arose in connection with the construction of power sequence terraces [1, 2, 3], we now introduce it independently of its provenance, with a brief illustration of the link between daisy chains and terraces in the final section of this paper.

Any positive integer  $n$  has a prime-power decomposition  $n = p^i q^j r^k \dots$  ( $i, j, k \geq 1$ ) where  $p, q, r, \dots$  are finitely many distinct primes. In standard number-theoretic terminology, the *units* of the corresponding group  $\mathbb{Z}_n$  are those elements of  $\mathbb{Z}_n \setminus \{0\}$  that are coprime with  $n$  (e.g. [14, p. 84]). The number of units in  $\mathbb{Z}_n$  is given by Euler’s totient function

$$\phi(n) = (p - 1)p^{i-1}(q - 1)q^{j-1}(r - 1)r^{k-1} \dots$$

(e.g. [14, p. 87]). For  $n$  odd, we define a *daisy chain* for the units of  $\mathbb{Z}_n$  to be an ordered arrangement  $[a_1, a_2, \dots, a_{\phi(n)}]$  of the units on a circle, such that the set of differences  $b_i = a_{i+1} - a_i$  ( $i = 1, 2, \dots, \phi(n)$ , with  $a_{\phi(n)+1} = a_1$ ) is itself the set of units. Here, as in [15], we use square brackets to indicate a cycle. (The terminology *daisy chain* has had other mathematical usages, but these were in mathematical areas so far removed from the present context that no confusion should arise.)

For convenience, we write a displayed daisy chain in linear form, without brackets and commas:

$$\hookrightarrow a_1 \ a_2 \ a_3 \ \dots \ a_{\phi(n)} \ \leftarrow \pmod n .$$

Here the symbols  $\hookrightarrow$  and  $\leftarrow$  are reminders that the two ends of the linear form are joined. We always regard the entry after the symbol  $\hookrightarrow$  as being  $a_1$ .

If  $n$  is an odd prime, the units of  $\mathbb{Z}_n$  comprise all the elements of  $\mathbb{Z}_n \setminus \{0\}$ . Thus

$$\hookrightarrow 1 \ 2 \ 5 \ 4 \ 6 \ 3 \ \leftarrow \pmod 7$$

is a daisy chain for the units of  $\mathbb{Z}_7$ , and

$$\hookrightarrow 1 \ 2 \ 4 \ 9 \ 6 \ 10 \ 5 \ 8 \ 7 \ 3 \ \leftarrow \pmod{11}$$

is a daisy chain for the units of  $\mathbb{Z}_{11}$ . These daisy chains were found by trial-and-error, but this paper gives a succession of systematic constructions for daisy chains. Each construction involves at least one sequence of successive powers of a unit of  $\mathbb{Z}_n$ , so our approach is similar to that used in [1, 2, 3] for constructing power-sequence terraces for  $\mathbb{Z}_n$ . Our emphasis is on values of  $n$  lying in the range  $1 < n < 300$ , so we consider only the cases  $n = p^i$  ( $i \geq 1$ ),  $n = p^i q^j$  ( $i \geq 1, j \geq 1$ ) and  $n = pqr$  where  $p, q$  and  $r$  are distinct odd primes.

For values of  $n$  that are odd prime powers, primitive roots of  $n$  can be used in constructing daisy chains (see Theorem 2.1 below). However, other odd integers greater than 1 do not have primitive roots. For these other values of  $n$ , the “next best thing” to a primitive root is a *primitive  $\lambda$ -root* of  $n$ , which is a unit of  $\mathbb{Z}_n$  that is of maximum order [8, 9], that order being given by Carmichael’s  $\lambda$ -function. As

the literature of primitive  $\lambda$ -roots is sparse, notes on them have been placed on the Web [7]. As in those notes, we write  $\lambda(n)$  for the order of a primitive  $\lambda$ -root of  $n$ , and we write  $\xi(n) = \phi(n)/\lambda(n)$ . For any composite odd  $n$ , the value of  $\xi(n)$  is even [7, §6]. A primitive  $\lambda$ -root  $x$  is *inward* if  $x - 1$  is a unit of  $\mathbb{Z}_n$ . A primitive  $\lambda$ -root  $x$  is *negating* if  $-1 \in \langle x \rangle$ .

We write  $\mathbb{U}_n$  for the set of units of  $\mathbb{Z}_n$ . Thus  $|\mathbb{U}_n| = \phi(n)$ . If  $z \in \mathbb{U}_n$ , we write  $\text{ord}_n(z)$  for the order of  $z$ , modulo  $n$ .

## 2 $n$ an odd prime power

If  $n$  is an odd prime [not prime power], a daisy chain for  $\mathbb{U}_n$  is also, as stated above, a directed R-terrace for  $\mathbb{Z}_n$ , for which the cycle of differences is an R-sequencing of  $\mathbb{Z}_n$  [13], a concept introduced in [16]. Such a daisy chain can therefore be obtained from the construction given by Friedlander, Gordon and Miller [11]:

$$\hookrightarrow a_1 \ a_2 \ \dots \ a_r \ a_r + r \ a_{r-1} + r \ \dots \ a_1 + r \ \leftarrow \pmod n$$

where  $r = (n - 1)/2$  and

$$a_i = \begin{cases} (i + 1)/2 & \text{if } i \text{ is odd,} \\ r + 1 - i/2 & \text{if } i \text{ is even.} \end{cases}$$

If  $n \equiv 3 \pmod 4$ , the sequence of differences for this daisy chain is the same as that obtained for one of the ‘total cycles’ constructed by Azaïs [4]; if  $n \equiv 1 \pmod 4$ , the two sequences of differences become the same if the Azaïs cycle is reversed.

Also, if  $n$  is a prime of the form  $12s + 7$ , a daisy chain (here again, a directed R-terrace) can be obtained as the log of a circuit of a current graph used to obtain a triangular rotation of  $K_n$ . The rotation scheme given by Ringel [18, p. 26] yields the following daisy chain for  $\mathbb{Z}_{19}$ :

$$\hookrightarrow 1 \ 11 \ 14 \ 13 \ 15 \ 3 \ 8 \ 9 \ 7 \ 4 \ 17 \ 10 \ 18 \ 5 \ 16 \ 12 \ 2 \ 6 \ \leftarrow,$$

whereas the recipe given by Youngs [19, again p. 26] yields

$$\hookrightarrow 1 \ 3 \ 7 \ 6 \ 14 \ 4 \ 16 \ 17 \ 9 \ 5 \ 11 \ 2 \ 18 \ 12 \ 15 \ 10 \ 8 \ 13 \ \leftarrow.$$

Further examples for primes  $n = 12s + 7$  ( $s = 1, 2, 3, 5, 6$ ) appear in [6, 12].

However, if  $n = p^i$  ( $i > 1$ ) where  $p$  is prime, a daisy chain for  $\mathbb{U}_n$  is not a directed R-terrace for  $\mathbb{Z}_n$ , nor can the above constructions be tweaked to produce daisy chains. Accordingly, we now give some seemingly new constructions for daisy chains for  $\mathbb{U}_n$  where  $n$  is an odd prime power  $n = p^i$  ( $i \geq 1$ ), the number of units being  $|\mathbb{U}_n| = \phi(n) = (p - 1)p^{i-1}$ .

**Theorem 2.1** *Let  $n$  be an odd prime power, and let  $x$  be a primitive root of  $n$ . Write  $2\pi = \phi(n) = \text{ord}_n(x)$ . Then*

$$\hookrightarrow x^0 \ x^1 \ x^2 \ \dots \ x^{2\pi-1} \ \leftarrow \pmod n$$

*is a daisy chain for  $\mathbb{U}_n$ .*

**Proof:** Trivial. □

**Example 2.1:** If we take  $n = 25$  then 3 is a primitive root of  $n$  and we have  $\pi = 20$ . Taking  $x = 3$  gives us the following daisy chain for  $\mathbb{U}_{25}$ :

$$\hookrightarrow 1 \ 3 \ 9 \ 2 \ 6 \ 18 \ 4 \ 12 \ 11 \ 8 \ 24 \ 22 \ 16 \ 23 \ 19 \ 7 \ 21 \ 13 \ 14 \ 17 \ \leftarrow .$$

**Theorem 2.2** *Let  $n$  be an odd prime power, and again write  $2\pi = \phi(n)$ . Let  $y$  be a unit of  $\mathbb{Z}_n$  that is of order  $\pi$ . Suppose that there is a further unit  $c$  in  $\mathbb{Z}_n$  such that  $c \notin \langle y \rangle$  and such that exactly one of  $c - 1$  and  $y - c$  lies in  $\langle y \rangle$  and the other lies in  $\mathbb{U}_n \setminus \langle y \rangle$ . Then*

$$\hookrightarrow y^0 \ cy^0 \ y^1 \ cy^1 \ y^2 \ cy^2 \ \dots \ y^{\pi-1} \ cy^{\pi-1} \ \leftarrow \pmod n$$

is a daisy chain for  $\mathbb{U}_n$ .

**Proof:** The differences  $b_1, b_3, \dots, b_{n-2}$  are  $(c - 1)y^0, (c - 1)y^1, \dots, (c - 1)y^{\pi-1}$ . Likewise, the differences  $b_2, b_4, \dots, b_{n-1}$  are  $(y - c)y^0, (y - c)y^1, \dots, (y - c)y^{\pi-1}$ . The result follows at once. □

**Note 2.2:** If we choose  $c$  so that  $c^2 = y$ , we obtain a special case of Theorem 2.1.

**Example 2.2(a):** For  $n = 11$ , take  $y = 9$  and  $c = 2$  in Theorem 2.2. Then  $c$  and  $y - c$  are quadratic non-residues, and  $c - 1$  is a quadratic residue. Thus we obtain the following daisy chain for  $\mathbb{U}_{11}$ :

$$\hookrightarrow 1 \ 2 \ 9 \ 7 \ 4 \ 8 \ 3 \ 6 \ 5 \ 10 \ \leftarrow .$$

**Example 2.2(b):** For  $n = 13$ , which has  $\pi = 6$ , take  $y = 4$  and  $c = 8$  in Theorem 2.2. Then  $c$  and  $c - 1$  are quadratic non-residues but  $y - c$  is a quadratic residue, so we obtain the following daisy chain for  $\mathbb{U}_{13}$ :

$$\hookrightarrow 1 \ 8 \ 4 \ 6 \ 3 \ 11 \ 12 \ 5 \ 9 \ 7 \ 10 \ 2 \ \leftarrow .$$

Here, as  $\pi$  is even and  $y^{\pi/2} \equiv -1 \pmod n$ , the difference at any position is the negative of the difference  $\pi$  positions later.

**Example 2.2(c):** For  $n = 25$ , take  $y = 4$  and  $c = 3$  in Theorem 2.2. Then  $c - 1 = 2 \in \mathbb{U}_n \setminus \langle 4 \rangle$ , whereas  $y - c = 1 \in \langle 4 \rangle$ . Thus we obtain the following daisy chain for  $\mathbb{U}_{25}$ :

$$\hookrightarrow 1 \ 3 \ 4 \ 12 \ 16 \ 23 \ 14 \ 17 \ 6 \ 18 \ 24 \ 22 \ 21 \ 13 \ 9 \ 2 \ 11 \ 8 \ 19 \ 7 \ \leftarrow .$$

**Example 2.2(d):** For  $n = 49$  we can take  $(y, c) = (9, 17)$  in Theorem 2.2.

We now come to a theorem that has analogues for values of  $n$  that are not prime powers. Each daisy chain obtained from this theorem (similar to Theorem 4.3 below) is made up of  $\pi$  segments each comprising  $\omega$  entries where  $\pi$  is some integer satisfying  $2 < \pi < (n - 1)/2$ . For clarity, the segments of the printed daisy chain are separated by vertical bars, referred to henceforth as *fences*.

**Theorem 2.3** *Let  $n$  be an odd prime power. Suppose that  $\phi(n) = \pi\omega$  where  $\pi$  and  $\omega$  are coprime ( $2 < \pi$  and  $2 < \omega$ ), so that exactly one of  $\pi$  and  $\omega$  is odd. Suppose further that there are units  $x$  and  $z = (x + 1)^{-1}$  in  $\mathbb{Z}_n$  such that  $\text{ord}_n(x) = \pi$  and  $\text{ord}_n(z) = \omega$ . Then*

$$\begin{aligned} \hookrightarrow x^0z^0 \ x^0z^1 \ \dots \ x^0z^{\omega-1} \mid x^1z^0 \ x^1z^1 \ \dots \ x^1z^{\omega-1} \mid \\ \dots \mid x^{\pi-1}z^0 \ x^{\pi-1}z^1 \ \dots \ x^{\pi-1}z^{\omega-1} \mid \leftarrow (\text{mod } n) \end{aligned}$$

is a daisy chain for  $\mathbb{U}_n$ .

**Proof:** Label the segments, in the above order, as S1, S2, . . . . We show that the difference  $1 - z^{\omega-1}$  that is missing from S1 equals the difference  $x^2 - xz^{\omega-1}$  across the second fence:

$$\begin{aligned} (1 - z^{\omega-1}) - (x^2 - xz^{\omega-1}) &= 1 - z^{-1} - x^2 + xz^{-1} \\ &= (x - 1)[z^{-1} - (x + 1)] \\ &\equiv 0 \pmod{n}. \quad \square \end{aligned}$$

**Coverage of Theorem 2.3:**

In the range  $1 < n < 300$ , Theorem 2.3 can be used to obtain daisy chains with parameters as follows:

$n$	$\pi$	$\omega$	$x$	$n$	$\pi$	$\omega$	$x$	$n$	$\pi$	$\omega$	$x$
13 <sup>†</sup>	4	3	8	125	25	4	56	223*	6	37	40
25	5	4	6	139*	6	23	43		74	3	182
29 <sup>†</sup>	7	4	16		46	3	95	229	19	12	17
37 <sup>†</sup>	4	9	6	149 <sup>†</sup>	37	4	104		76	3	93
41	5	8	37	157	12	13	107	233	29	8	135
53 <sup>†</sup>	4	13	23	173 <sup>†</sup>	4	43	80	239*	14	17	215
61 <sup>†</sup>	4	15	11	181 <sup>†</sup>	9	20	73		34	7	23
	5	12	20		45	4	161	241	5	48	87
71*	5	14	25	191*	10	19	152		80	3	224
	7	10	45		38	5	38	269 <sup>†</sup>	67	4	81
89	8	11	77		5	38	184	277	92	3	159
97	32	3	34		19	10	6	283*	6	47	239
101 <sup>†</sup>	4	25	91	197 <sup>†</sup>	49	4	182		94	3	43
113	16	7	48	199*	9	22	180	293 <sup>†</sup>	73	4	137
					11	18	18				

<sup>†</sup>  $n \equiv 5 \pmod{8}$ ; 2 is a primitive root of  $n$

\*  $n \equiv 3 \pmod{4}$ ; the two  $x$ -values in each pair of daisy chains sum to  $n - 1$

**Example 2.3(a):** For  $n = 13$  we can use  $x = 8$  in Theorem 2.3 to obtain the following daisy chain for  $\mathbb{U}_{13}$ :

$$\hookrightarrow 1 \ 3 \ 9 \mid 8 \ 11 \ 7 \mid 12 \ 10 \ 4 \mid 5 \ 2 \ 6 \ \leftarrow .$$

**Example 2.3(b):** For  $n = 25$  we have  $\phi(n) = 20$  and we can use  $x = 6$  in Theorem 2.3 to obtain the following daisy chain for  $\mathbb{U}_{25}$ ;

$$\begin{aligned} \hookrightarrow 1 \ 18 \ 24 \ 7 \mid 6 \ 8 \ 19 \ 17 \mid 11 \ 23 \ 14 \ 2 \mid \\ 16 \ 13 \ 9 \ 12 \mid 21 \ 3 \ 4 \ 22 \ \leftarrow . \end{aligned}$$

As a value  $x$  satisfying the conditions of Theorem 2.3 does not exist for all odd prime powers  $n$  with  $\phi(n) = \pi\omega$  where  $\phi$  and  $\omega$  are coprime and each greater than 2, we now weaken Theorem 2.3 by replacing  $z$  by a unit  $y$  with  $\phi(n) \leq \pi \operatorname{ord}_n(y)$ .

**Theorem 2.4** *Let  $n$  be an odd prime power. Suppose that there are units  $x$  and  $y$  of  $\mathbb{Z}_n$  such that  $\mathbb{U}_n = \langle x, y \rangle$  with  $1 < \pi = \operatorname{ord}_n(x) < |\mathbb{U}_n|/2$  and  $\omega = |\mathbb{U}_n|/\pi \leq \operatorname{ord}_n(y) \leq |\mathbb{U}_n|$ . If  $(x - y^{\omega-1})\langle x \rangle = (y - 1)y^{\omega-1}\langle x \rangle$ , then*

$$\begin{aligned} \hookrightarrow x^0y^0 \ x^0y^1 \ \dots \ x^0y^{\omega-1} \mid x^1y^0 \ x^1y^1 \ \dots \ x^1y^{\omega-1} \mid \\ \dots \mid x^{\pi-1}y^0 \ x^{\pi-1}y^1 \ \dots \ x^{\pi-1}y^{\omega-1} \mid \leftarrow \pmod n \end{aligned}$$

is a daisy chain for  $\mathbb{U}_n$ .

**Proof:** The differences arising from the  $\ell^{\text{th}}$  segment ( $\ell = 1, 2, \dots, \pi$ ) are

$$x^{\ell-1}y^0(y - 1), x^{\ell-1}y^1(y - 1), \dots, x^{\ell-1}y^{\omega-2}(y - 1)$$

and the fence difference at the end of the  $\ell^{\text{th}}$  segment is  $x^{\ell-1}(x - y^{\omega-1})$ . The result follows at once. □

**Examples 2.4(a):** For  $n = 25$  we can take  $(x, y) = (6, 2)$  in Theorem 2.4. Then  $\pi = \operatorname{ord}_n(x) = 5$  and  $\operatorname{ord}_n(y) = |\mathbb{U}_n| = 20$ , so that  $\omega = 4$ . With these values we obtain the following daisy chain for  $\mathbb{U}_{25}$ :

$$\begin{aligned} \hookrightarrow 1 \ 2 \ 4 \ 8 \mid 6 \ 12 \ 24 \ 23 \mid 11 \ 22 \ 19 \ 13 \mid \\ 16 \ 7 \ 14 \ 3 \mid 21 \ 17 \ 9 \ 18 \mid \leftarrow . \end{aligned}$$

**Example 2.4(b):** In Theorem 2.4 take  $n = 31$  (a value not covered by Theorem 2.3) with  $(x, y) = (8, 3)$ . Then  $\operatorname{ord}_n(y) = |\mathbb{U}_n|$ , with  $\pi = 5$  and  $\omega = 6$ . We obtain the following daisy chain for  $\mathbb{U}_{31}$ :

$$\begin{aligned} \hookrightarrow 1 \ 3 \ 9 \ 27 \ 19 \ 26 \mid 8 \ 24 \ 10 \ 30 \ 28 \ 22 \mid 2 \ 6 \ 18 \ 23 \ 7 \ 21 \mid \\ 16 \ 17 \ 20 \ 29 \ 25 \ 13 \mid 4 \ 12 \ 5 \ 15 \ 14 \ 11 \mid \leftarrow . \end{aligned}$$

### 3 $n = p^i q^j$ with $\xi(n) = 2$

Theorem 2.2 can readily be adapted as follows for  $n$ -values that satisfy  $n = p^i q^j$  and  $\xi(n) = 2$ .

**Theorem 3.1** Let  $n = p^i q^j$  ( $i \geq 1, j \geq 1$ ) where  $p$  and  $q$  are distinct odd primes such that  $\gcd((p-1)p^{i-1}, (q-1)q^{j-1}) = 2$ . Let  $y$  be a primitive  $\lambda$ -root of  $n$ . Write  $\pi = \text{ord}_n(y) = \text{lcm}((p-1)p^{i-1}, (q-1)q^{j-1})$ . Suppose that there is a further unit  $c$  in  $\mathbb{Z}_n$  such that  $c \notin \langle y \rangle$  and such that exactly one of  $c-1$  and  $y-c$  lies in  $\langle y \rangle$  and the other lies in  $\mathbb{U}_n \setminus \langle y \rangle$ . Then

$$\hookrightarrow y^0 \quad cy^0 \quad y^1 \quad cy^1 \quad y^2 \quad cy^2 \quad \dots \quad y^{\pi-1} \quad cy^{\pi-1} \hookleftarrow \pmod n$$

is a daisy chain for  $\mathbb{U}_n$ .

**Proof:** As before. □

**Example 3.1(a):** For  $n = 33$  we have  $\pi = \text{lcm}(2, 10) = 10$ . To meet Theorem 3.1's requirements on  $c-1$  and  $y-c$  we need  $c \equiv 2 \pmod 3$  and  $y \equiv 1 \pmod 3$ . These requirements can be met by, for example, taking  $(y, c) = (28, 5)$ , whence we obtain the following daisy chain for  $\mathbb{U}_{33}$ :

$$\hookrightarrow 1 \ 5 \ 28 \ 8 \ 25 \ 26 \ 7 \ 2 \ 31 \ 23 \ 10 \ 17 \ 16 \ 14 \ 19 \ 29 \ 4 \ 20 \ 13 \ 32 \ \hookleftarrow .$$

**Example 3.1(b):** For  $n = 45$  we can in Theorem 3.1 take  $n = p^2 q$  where  $p = 3$  and  $q = 5$ , and we have  $\pi = 12$ . We can, for example, take  $y = 13$  and  $c = 2$ , as these give us  $y-c \notin \langle 13 \rangle$ .

**Note 3.1:** An important special case of Theorems 2.2 and 3.1 arises when we can take  $y = c-1 = -2$ . The daisy chain then becomes

$$\hookrightarrow +1 \quad -1 \quad -2 \quad +2 \quad +4 \quad -4 \quad -8 \quad +8 \quad \dots \ \hookleftarrow \pmod n .$$

In the range  $1 < n < 300$  this choice can be used for the following values of  $n$ :

$n$  prime,  $n \equiv 3 \pmod 8$ :-

- 11, 19, 59, 67, 83, 107, 131, 139, 163, 179, 211, 227;

$n$  composite:-

- 15, 21, 35, 39, 45, 55, 69, 75, 77, 87, 95,
- 111, 115, 141, 143, 159, 183, 203, 235, 253, 295, 299.

#### 4 $n = p^i q^j$ with $\xi(n) \geq 4$

For  $n$ -values that satisfy  $n = p^i q^j$ , the case  $\xi(n) = 4$  is sufficiently important and sufficiently distinctive to deserve special attention, and it is for this case that we give our next theorem. In this section of the paper we use the symbol  $x$  for a primitive  $\lambda$ -root of  $n$ , which is why the first two theorems have the power of  $z$ , not  $x$ , constant within a segment.

**Theorem 4.1** Let  $n$  be an integer of the form  $n = p^i q^j$  ( $i \geq 1, j \geq 1$ ) where  $p$  and  $q$  are distinct odd primes. Suppose that  $\xi(n) = 4$ . Suppose further that  $x$  is an inward

primitive  $\lambda$ -root of  $n$  such that there is a unit  $z$  of  $\mathbb{Z}_n$  that satisfies  $z \equiv x^{-1} - 1$  and  $z^4 \equiv +1 \pmod{n}$ , with  $\mathbb{U}_n = \langle x, z \rangle$ . Write  $\text{ord}_n(x) = \pi$ . Then

$$\begin{aligned} &\hookrightarrow x^0 \ x^1 \ \dots \ x^{\pi-1} \mid zx^0 \ zx^1 \ \dots \ zx^{\pi-1} \mid \\ &z^2x^0 \ z^2x^1 \ \dots \ z^2x^{\pi-1} \mid z^3x^0 \ z^3x^1 \ \dots \ z^3x^{\pi-1} \mid \leftrightarrow \pmod{n} \end{aligned}$$

is a daisy chain for  $\mathbb{U}_n$ .

**Proof:** As Theorem 2.3. □

**Note 4.1(a):** If  $x$  and  $z$  in Theorem 4.1 can take the values  $x_1$  and  $z_1$  respectively, then they can also take the values  $x_2$  and  $z_2$  respectively, where  $x_2 \equiv x_1z_1 \equiv 1 - x_1$  and  $z_2 \equiv z_1^{-1} \pmod{n}$ . This is because, firstly,

$$\begin{aligned} z_2 - (x_2^{-1} - 1) &= z_1^{-1} - (x_1^{-1}z_1^{-1} - 1) \\ &= z_1^{-1}[z_1 - (x_1^{-1} - 1)] \\ &\equiv 0 \pmod{n}. \end{aligned}$$

Secondly, the fact that  $x_1$  is a primitive  $\lambda$ -root of  $n$  implies that  $\text{ord}_n(x_2) = \text{ord}_n(x_1z_1) = \text{ord}_n(x_1)$ , whence  $x_2$  is also a primitive  $\lambda$ -root of  $n$ . Thirdly, as  $x_1$  is inward,  $x_1$  and  $x_1 - 1$  are units; thus  $x_2$  and  $x_2 - 1$ , given by  $1 - x_1$  and  $-x_1$  respectively, are units too, whence  $x_2$  is inward. No analogous result applies for Theorem 2.3.

**Note 4.1(b):** If  $(x, z)$  can take the values  $(x_1, z_1)$  and  $(x_2, z_2)$  as above, and  $z_1^2 \equiv z_2^2 \equiv -1 \pmod{n}$ , then

$$\begin{aligned} z_1 + z_2 &= z_1 + z_1^{-1} \\ &= z_1^{-1}(z_1^2 + 1) \\ &\equiv 0 \pmod{n}, \end{aligned}$$

so that  $z_1 \equiv z_2^{-1} \equiv -z_2 \pmod{n}$ .

**Coverage of Theorem 4.1:** If  $n = pq$  in Theorem 4.1 we have  $\xi(n) = \text{gcd}(p - 1, q - 1) = 4$ , whence  $p$  and  $q$  must both be congruent to 1, modulo 4, whereas they cannot both be congruent to 1, modulo 8. For many such  $n$ -values, Theorems 8.5 and 8.6 of [7] provide admissible duples  $(x, z)$  with  $z^2 \equiv -1 \pmod{n}$ . However, we can also have  $z^2 \not\equiv -1 \pmod{n}$ . The following table gives details of the possibilities for  $n$ -values satisfying  $1 < n < 300$ . Any value of  $x$  or  $z$  that generates  $-1$  is marked with an asterisk \*. The four duples marked with a dagger † have  $z \equiv 2x \pmod{n}$ , which implies  $(z - 1)(x + 1) \equiv 0 \pmod{n}$ . Pairs of duples that are related as in Note 4.1(a) are listed together in square brackets.



$(n, p, q)$	$(x, z)$		
	$z^2 \equiv -1 \pmod{n}$ (see Note 4.1(b))	$z^2 \equiv +1 \pmod{p}$ $z^2 \equiv -1 \pmod{q}$	$z^2 \equiv +1 \pmod{q}$ $z^2 \equiv -1 \pmod{p}$
$(65, 5, 13)$	$[(24, 18^*), (42, 47^*)]$	$[(3, 21), (63^*, 31)]$	$[(59, 53)^\dagger, (7^*, 27)]$
$(85, 5, 17)$	$\left\{ \begin{array}{l} [(79, 13^*), (7, 72^*)], \\ [(24, 38^*), (62, 47^*)] \end{array} \right.$	—	—
$(145, 5, 29)$	$[(67, 12^*), (79, 133^*)]$	$[(38, 41), (108^*, 46)]$	$[(44, 88)^\dagger, (102^*, 117)]$
$(185, 5, 37)$	$[(59, 68^*), (127, 117^*)]$	$[(53, 6), (133^*, 31)]$	$[(19, 38)^\dagger, (167^*, 112)]$
$(205, 5, 41)$	—	—	—
$(221, 13, 17)$	$\left\{ \begin{array}{l} [(211, 21^*), (11, 200^*)], \\ [(198, 47^*), (23, 174^*)] \end{array} \right.$	—	—
$(265, 5, 53)$	$[(224, 83^*), (42, 182^*)]$	$[(148, 76), (118^*, 136)]$	$[(239, 213)^\dagger, (27^*, 107)]$

**Examples 4.1(a):** For  $n = 65$  we present in full three examples from Theorem 4.1, to give readers the feel of different types. First we give the  $\mathbb{U}_{65}$  daisy chain for  $(x, z) = (42, 47^*)$ . In this, any 24 consecutive entries are the negatives of the next 24 consecutive entries:

$$\begin{aligned} \hookrightarrow & 1 \ 42 \ 9 \ 53 \ 16 \ 22 \ 14 \ 3 \ 61 \ 27 \ 29 \ 48 \ | \\ & 47 \ 24 \ 33 \ 21 \ 37 \ 59 \ 8 \ 11 \ 7 \ 34 \ 63 \ 46 \ | \\ & 64 \ 23 \ 56 \ 12 \ 49 \ 43 \ 51 \ 62 \ 4 \ 38 \ 36 \ 17 \ | \\ & 18 \ 41 \ 32 \ 44 \ 28 \ 6 \ 57 \ 54 \ 58 \ 31 \ 2 \ 19 \ | \ \leftarrow . \end{aligned}$$

Now we give the daisy chain for  $(x, z) = (3, 21)$ :

$$\begin{aligned} \hookrightarrow & 1 \ 3 \ 9 \ 27 \ 16 \ 48 \ 14 \ 42 \ 61 \ 53 \ 29 \ 22 \ | \\ & 21 \ 63 \ 59 \ 47 \ 11 \ 33 \ 34 \ 37 \ 46 \ 8 \ 24 \ 7 \ | \\ & 51 \ 23 \ 4 \ 12 \ 36 \ 43 \ 64 \ 62 \ 56 \ 38 \ 49 \ 17 \ | \\ & 31 \ 28 \ 19 \ 57 \ 41 \ 58 \ 44 \ 2 \ 6 \ 18 \ 54 \ 32 \ | \ \leftarrow . \end{aligned}$$

Here, for any  $i$ , the entries in the first half of the  $i^{\text{th}}$  segment are the negatives of the respective entries in the second half of the  $(i + 2)^{\text{th}}$  segment. Last, the daisy chain for  $(x, z) = (7^*, 27)$ :

$$\begin{aligned} \hookrightarrow & 1 \ 7 \ 49 \ 18 \ 61 \ 37 \ 64 \ 58 \ 16 \ 47 \ 4 \ 28 \ | \\ & 27 \ 59 \ 23 \ 31 \ 22 \ 24 \ 38 \ 6 \ 42 \ 34 \ 43 \ 41 \ | \\ & 14 \ 33 \ 36 \ 57 \ 9 \ 63 \ 51 \ 32 \ 29 \ 8 \ 56 \ 2 \ | \\ & 53 \ 46 \ 62 \ 44 \ 48 \ 11 \ 12 \ 19 \ 3 \ 21 \ 17 \ 54 \ | \ \leftarrow . \end{aligned}$$

Here, a negating primitive  $\lambda$ -root is used, and the entries in the first half of any segment are the negatives of the respective entries in the second half.

**Example 4.1(b):** The  $n$ -value  $325 = 5^2 \times 13$ , although outside the range  $1 < n < 300$  on which this paper concentrates, merits special attention. It is not covered by Theorems 8.5 and 8.6 of [7] (see above) as these, like the table above, are restricted

to  $n$ -values with  $n = pq$ . However, little imagination is needed to generalise the Cameron-and-Preece theorems [7] to other cases with  $n = p^i q^j$  and  $\xi(n) = 4$ . For  $n = 325$  we can, for example, take  $(x, z) = (172, 307^*)$  to obtain the following daisy chain for  $\mathbb{U}_{325}$ :

$$\begin{aligned} \hookrightarrow & \underbrace{1 \ 172 \ \dots \ 308}_{60 \text{ terms}} \mid \underbrace{307 \ 154 \ \dots \ 306}_{60 \text{ terms}} \mid \\ & \underbrace{324 \ 153 \ \dots \ 17}_{60 \text{ terms}} \mid \underbrace{18 \ 171 \ \dots \ 19}_{60 \text{ terms}} \mid \leftrightarrow \dots \end{aligned}$$

If the values  $(x, z)$  here are reduced modulo 65, we have  $(42, 47)$  as in the first of Examples 4.1(a), but  $47^2 \not\equiv -1 \pmod{325}$ .

We now generalise Theorem 4.1 to cover  $\xi(n) \geq 4$ . As before,  $p$  and  $q$  are distinct odd primes.

**Theorem 4.2** *Let  $n$  be a positive integer of the form  $n = p^i q^j$  ( $i \geq 1, j \geq 1$ ) such that  $\omega = \xi(n) \geq 4$ . Let  $x$  be an inward primitive  $\lambda$ -root of  $n$  and let  $z$  be a unit of  $\mathbb{Z}_n$  that satisfies  $\mathbb{U}_n = \langle x, z \rangle$  and  $z^\omega \equiv +1 \pmod{n}$ . Suppose that  $(z-1)[z-(x^{-1}-1)] \equiv 0 \pmod{n}$ . Write  $\text{ord}_n(x) = \pi$ . Then*

$$\begin{aligned} \hookrightarrow & z^0 x^0 \quad z^0 x^1 \quad \dots \quad z^0 x^{\pi-1} \mid z^1 x^0 \quad z^1 x^1 \quad \dots \quad z^1 x^{\pi-1} \mid \\ & \dots \mid z^{\omega-1} x^0 \quad z^{\omega-1} x^1 \quad \dots \quad z^{\omega-1} x^{\pi-1} \mid \leftrightarrow \pmod{n} \end{aligned}$$

is a daisy chain for  $\mathbb{U}_n$ .

**Proof:** As for Theorem 4.1. □

**Note 4.2:** If  $x$  and  $z$  in Theorem 4.2 can take the values  $x_1$  and  $z_1$  respectively, then they can also take the values  $x_2$  and  $z_2$  respectively, where  $x_2 = x_1 z_1$  and  $z_2 = z_1^{-1}$ . This is because, firstly,

$$\begin{aligned} (z_2 - 1)[z_2 - (x_2^{-1} - 1)] &= (z_1^{-1} - 1)[z_1^{-1} - (x_1^{-1} z_1^{-1} - 1)] \\ &= -z_1^{-2}(z_1 - 1)(1 - x_1^{-1} + z_1) \\ &= -z_1^{-2}(z_1 - 1)[z_1 - (x_1^{-1} - 1)] \\ &\equiv 0 \pmod{n}. \end{aligned}$$

Secondly, as in Note 4.1(a), the fact that  $x_1$  is a primitive  $\lambda$ -root of  $n$  implies that  $x_2$  is a primitive  $\lambda$ -root too. Finally, as  $x_1$  is inward,  $x_1$  and  $x_1 - 1$  are units. Thus  $x_2$ , given by  $x_2 = x_1 z_1$ , is a unit. Also

$$\begin{aligned} 0 &\equiv (z_1 - 1)[z_1 - (x_1^{-1} - 1)] \\ & \quad (z_1 - 1)x_1^{-1}[(x_1 z_1 - 1) + x_1] \\ & \quad (z_1 - 1)x_1^{-1}[(x_2 - 1) + x_1] \pmod{n}, \end{aligned}$$

whence  $x_2 - 1$  must also be a unit. Thus  $x_2$  is inward too.

**Coverage of Theorem 4.2:** Even for  $n$ -values in the range  $1 < n < 300$ , with  $\xi(n) > 4$ , there are many pairs  $(x, z)$  that satisfy the conditions of Theorem 4.2. So the following table is restricted to possibilities that have  $z \equiv x^{-1} - 1 \pmod n$ . An asterisk  $*$  again marks a value that generates  $-1$ , and a dagger  $\dagger$  signifies  $z \equiv 2x \pmod n$ .

$n$	$\xi(n)$	duples $(x, z)$
$63 = 3^2 \cdot 7$	6	$[(44, 52), (20^*, 40)^\dagger], [(23, 10), (41^*, 19)^\dagger]$
$91 = 7 \cdot 13$	6	$[(86, 17^*), (6, 75^*)], [(72, 66), (20, 40)^\dagger]$
$117 = 3^2 \cdot 13$	6	—
$133 = 7 \cdot 19$	6	$[(79, 31^*), (55, 103^*)], [(86, 115), (48^*, 96)^\dagger],$ $[(17, 46), (117, 107)], [(131, 65), (3^*, 88)]$
$171 = 3^2 \cdot 19$	6	$[(17, 160), (155^*, 31)], [(74, 103), (98^*, 88)]$
$189 = 3^3 \cdot 7$	6	$[(86, 10), (104^*, 19)^\dagger], [(23, 73), (167^*, 145)^\dagger],$ $[(149, 136), (41^*, 82)^\dagger]$
$217 = 7 \cdot 31$	6	$[(195, 68^*), (23, 150^*)], [(164, 130), (54^*, 212)],$ $[(40, 37), (178^*, 88)]$
$247 = 13 \cdot 19$	6	$[(60, 69^*), (188, 179^*)], [(136, 88^*), (112, 160^*)]$
$259 = 7 \cdot 37$	6	$[(93, 38), (167, 75)^\dagger]$
$275 = 5^2 \cdot 11$	10	$[(38 + 55s, 151 + 55s), (238 - 55s, 51 - 55s)]$ $(s = 0, 1, 2, 4)$ $[(8 + 55s, 171 + 55s), (268 - 55s, 156 - 55s)]$ $(s = 0, 1, 2, 3, 4)$
$279 = 3^2 \cdot 31$	6	$[(71, 223), (209^*, 274)], [(257, 37), (23^*, 181)]$

**Example 4.2:** For  $n = 63$ , taking  $(x, z) = (41^*, 19)^\dagger$  in Theorem 4.2 yields the following daisy chain for  $\mathbb{U}_{63}$ :

$$\begin{aligned} \hookrightarrow & 1 \ 41 \ 43 \ 62 \ 22 \ 20 \mid 19 \ 23 \ 61 \ 44 \ 40 \ 2 \mid 46 \ 59 \ 25 \ 17 \ 4 \ 38 \mid \\ & 55 \ 50 \ 34 \ 8 \ 13 \ 29 \mid 37 \ 5 \ 16 \ 26 \ 58 \ 47 \mid 10 \ 32 \ 52 \ 53 \ 31 \ 11 \mid \leftrightarrow . \end{aligned}$$

Theorem 4.2 requires the difference missing from the first segment of its daisy chains to equal the difference across the **second** fence. Accordingly, if  $\xi(n) = 4$ , we can read such a daisy chain backwards to obtain one where the difference missing from the first segment equals the difference across the **third** fence. But if  $\xi(n) \geq 6$ , can we have a daisy chain as in Theorem 4.2 save that the first segment's missing difference equals the difference across the third fence? In general, yes. The congruence to be

satisfied jointly by  $x^{-1}$  and  $z$  is now

$$(z - 1)[(z + 1)(x^{-1} - 1) - z^2] \equiv 0 \pmod{n} .$$

For  $n$ -values satisfying  $n = pq$  and  $\xi(n) = 6$  in the range  $1 < n < 300$ , daisy chains can be obtained from the following duples  $(x, z)$  that satisfy the new congruence and the other necessary conditions from Theorem 4.2; square brackets and asterisks are used as before:

$n$	$(x, z)$
91 = 7 · 13	[(2 + 7s, 40), (80 + 7s, 66)] (s = 0, 5, 8, 10)
133 = 7 · 19	[(2 + 7s, 96), (59 + 7s*, 115)] (s = 0, 7, 10, 11, 12, 18)
217 = 7 · 31	[(19 + 31s, 57), (215 + 31s*, 99)] (s = 0, 4)
247 = 13 · 19	—
259 = 7 · 37	[(2 + 7s, 75), (150 + 7s, 38)] (s = 0, 10, 11, 13, 18, 19, 23, 24, 28, 29, 34, 36)

Likewise, for  $n = 275$ , which has  $\xi(n) = 10$ , we have found daisy chains as in Theorem 4.2 save that the first segment’s missing difference is equal to the difference across either the 4<sup>th</sup> or 5<sup>th</sup> fence.

We now reverse the roles of  $x$  and  $z$  in Theorem 4.1 to give the following:

**Theorem 4.3** *Let  $n$  be a positive integer of the form  $n = p^i q^j$  ( $i \geq 1, j \geq 1$ ) such that  $\xi(n) = 4$ . Suppose that  $x$  and  $z - 1$  are primitive  $\lambda$ -roots of  $n$  such that  $z^4 \equiv +1$  and  $x \equiv z^{-1} - 1 \pmod{n}$  and  $\mathbb{U}_n = \langle z, x \rangle$ . Write  $\text{ord}_n(x) = \pi$ . Then*

$$\begin{aligned} \hookrightarrow z^0 z^1 z^2 z^3 \mid xz^0 xz^1 xz^2 xz^3 \mid x^2z^0 x^2z^1 x^2z^2 x^2z^3 \mid \\ \dots \mid x^{\pi-1}z^0 x^{\pi-1}z^1 x^{\pi-1}z^2 x^{\pi-1}z^3 \mid \leftrightarrow \pmod{n} \end{aligned}$$

is a daisy chain for  $\mathbb{U}_n$ .

**Proof:** As for Theorem 2.3. □

**Note 4.3(a):** If  $z$  and  $x$  can take the values  $z_1$  and  $x_1$  respectively, then they can also take the values  $z_2$  and  $x_2$  respectively, where  $z_2 = x_1 + 1 = z_1^{-1}$  and  $x_2 = z_1 - 1$ . This is because

$$\begin{aligned} x_2 - (z_2^{-1} - 1) &= (x_2 + 1) - z_2^{-1} \\ &= z_1 - (x_1 + 1)^{-1} \\ &\equiv 0 \pmod{n} \end{aligned}$$

as  $z_1^{-1} \equiv x_1 + 1 \pmod{n}$ .

**Note 4.3(b):** If  $(z, x)$  can take the values  $(z_1, x_1)$  and  $(z_2, x_2)$  as above, and  $z_1^2 \equiv z_2^2 \equiv -1 \pmod{n}$ , then  $x_1 + x_2 = (z_2 - 1) + (z_1 - 1) = (z_1 + z_2) - 2 \equiv -2 \pmod{n}$ , by Note 4.3(b), by Note 4.1(b).

**Coverage of Theorem 4.3:** The following table provides details of the possible duples  $(z, x)$  for  $n$ -values satisfying  $1 < n < 300$ . Asterisks are used as before. The duples now marked with a dagger † have  $x \equiv 2z \pmod n$ , which implies  $(x - 1)(z + 1) \equiv 0 \pmod n$ . Pairs of duples that are related as in Note 4.3(a) are listed together in square brackets.

$(n, p, q)$	$(z, x)$		
	$z^2 \equiv -1 \pmod n$ (see Note 4.3(b))	$z^2 \equiv +1 \pmod p$ $z^2 \equiv -1 \pmod q$	$z^2 \equiv +1 \pmod q$ $z^2 \equiv -1 \pmod p$
(65, 5, 13)	[(18*, 46), (47*, 17)]	[(34, 43), (44, 33*)]	[(38, 11)†, (12, 37*)]
(85, 5, 17)	{ [(13*, 71), (72*, 12)], [(38*, 46), (47*, 37)]	—	—
(145, 5, 29)	[(12*, 132), (133*, 11)]	[(99, 103), (104, 98*)]	[(28, 56)†, (57, 27*)]
(185, 5, 37)	[(68*, 116), (117*, 67)]	[(154, 178), (179, 153*)]	[(73, 146)†, (147, 72*)]
(205, 5, 41)	—	—	—
(221, 13, 17)	{ [(21*, 199), (200*, 20)], [(47*, 173), (174*, 46)]	—	—
(265, 5, 53)	[(83*, 181), (182*, 82)]	[(129, 188), (189, 128*)]	[(158, 51)†, (52, 157*)]

**Example 4.3:** For  $n = 65$ , taking  $(z, x) = (44, 33^*)$  in Theorem 4.3 gives the following daisy chain with  $x \equiv 2^{-1} \pmod n$ :

$$\begin{aligned} \hookrightarrow & 1 \ 44 \ 51 \ 34 \mid 33 \ 22 \ 58 \ 17 \mid 49 \ 11 \ 29 \ 41 \mid 57 \ 38 \ 47 \ 53 \mid \\ & 61 \ 19 \ 56 \ 59 \mid 63 \ 42 \ 28 \ 62 \mid 64 \ 21 \ 14 \ 31 \mid 32 \ 43 \ 7 \ 48 \mid \\ & 16 \ 54 \ 36 \ 24 \mid 8 \ 27 \ 18 \ 12 \mid 4 \ 46 \ 9 \ 6 \mid 2 \ 23 \ 37 \ 3 \mid \hookleftarrow . \end{aligned}$$

By reversing the roles of  $x$  and  $z$  in Theorem 4.2 we could now generalise Theorem 4.3 to  $n$ -values with  $\xi(n) = \omega \geq 4$  where  $n = p^i q^j$  ( $i \geq 1, j \geq 1$ ), the integers  $p$  and  $q$  being distinct odd primes. However, the restriction  $z^\omega \equiv +1 \pmod n$  in Theorem 4.3 can be relaxed to  $y^\tau \equiv +1 \pmod n$  for some  $y$  with  $\tau > \omega$ . We now proceed using the relaxed restriction.

**Theorem 4.4** *Let  $n$  be a positive integer of the form  $n = p^i q^j$  ( $i \geq 1, j \geq 1$ ) such that  $\omega = \xi(n) \geq 4$ . Let  $x$  be a primitive  $\lambda$ -root of  $n$ , and let  $y$  be a unit from  $\mathbb{Z}_n$  such that  $y - 1 \in \mathbb{U}_n = \bigcup_{k=0}^{\omega-1} y^k \langle x \rangle$ . Thus  $\text{ord}_n(y) \geq \omega$ . As before, write  $\text{ord}_n(x) = \pi$ , so that  $|\mathbb{U}_n| = \omega\pi$ . If  $(x - y^{\omega-1}) \langle x \rangle = (y - 1)y^{\omega-1} \langle x \rangle$ , then the chain*

$$\begin{aligned} \hookrightarrow & x^0 y^0 \ x^0 y^1 \ \dots \ x^0 y^{\omega-1} \mid x^1 y^0 \ x^1 y^1 \ \dots \ x^1 y^{\omega-1} \mid \\ & \dots \mid x^{\pi-1} y^0 \ x^{\pi-1} y^1 \ \dots \ x^{\pi-1} y^{\omega-1} \mid \hookleftarrow \pmod n \end{aligned}$$

(as in Theorem 2.4) is a daisy chain for  $\mathbb{U}_n$ .

**Proof:** Almost as for Theorem 2.4. □

**Coverage of Theorem 4.4:** For the range  $1 < n < 300$ , the following table gives specimen values of  $(y, x)$  with  $\text{ord}_n(y) > \omega$ . (This last restriction cannot be satisfied for  $n = 63$ .)

$n$	$\xi(n)$	$(y, x)$	$n$	$\xi(n)$	$(y, x)$
$65 = 5 \cdot 13$	4	(2, 42)	$205 = 5 \cdot 41$	4	(2, 22)
$85 = 5 \cdot 17$	4	(2, 22)	$217 = 7 \cdot 31$	6	(44, 131)
$91 = 7 \cdot 13$	6	(5, 2)	$221 = 13 \cdot 17$	4	(2, 198)
$117 = 3^2 \cdot 13$	6	(2, 7)	$247 = 13 \cdot 19$	6	(51, 193)
$133 = 7 \cdot 19$	6	(2, 73)	$259 = 7 \cdot 37$	6	(5, 72)
$145 = 5 \cdot 29$	4	(3, 63)	$265 = 5 \cdot 53$	4	(2, 122)
$171 = 3^2 \cdot 19$	6	(2, 154)	$275 = 5^2 \cdot 11$	10	(42, 138)
$185 = 5 \cdot 37$	4	(2, 77)	$279 = 3^2 \cdot 31$	6	(2, 55)
$189 = 3^3 \cdot 7$	6	(2, 52)			

**Example 4.4:** For  $n = 65$  the duple  $(y, x) = (2, 42)$  yields the daisy chain  
 $\leftrightarrow 1 \ 2 \ 4 \ 8 \mid 42 \ 19 \ 38 \ 11 \mid 9 \ 18 \ 36 \ 7 \mid 53 \ 41 \ 17 \ 34 \mid$   
 $16 \ 32 \ 64 \ 63 \mid 22 \ 44 \ 23 \ 46 \mid 14 \ 28 \ 56 \ 47 \mid 3 \ 6 \ 12 \ 24 \mid$   
 $61 \ 57 \ 49 \ 33 \mid 27 \ 54 \ 43 \ 21 \mid 29 \ 58 \ 51 \ 37 \mid 48 \ 31 \ 62 \ 59 \mid \leftrightarrow .$

**5**  $n = pqr$  or  $n = p^i q^j$

Most of the procedures used so far, in this paper, are clearly inapplicable if  $n = pqr$  where  $p, q$  and  $r$  are distinct odd primes, as a multiplication table for  $\mathbb{U}_n$  for such an  $n$ -value must have at least three generators. However, we now introduce a general construction that covers (a) all such  $n$ -values in the range  $1 < n < 300$ , and (b) some other  $n$ -values already considered above.

**Theorem 5.1** *Let  $n$  be a positive integer  $n = p^i q^j$  ( $i \geq 1, j \geq 1$ ) or  $n = pqr$  (where  $p, q$  and  $r$  are distinct odd primes) such that  $\xi(n) \geq 4$ . Let  $x$  be a non-negating primitive  $\lambda$ -root of  $n$ . Write  $\sigma = \xi(n)/2$  and  $\text{ord}_n(x) = \pi$ , so that  $|\mathbb{U}_n| = 2\pi\sigma$ . Suppose that  $x$  is such that the  $2\sigma$  sets  $2^k \langle x \rangle$  and  $-2^k \langle x \rangle$  ( $k = 0, 1, \dots, \sigma - 1$ ) have zero intersection and union  $\mathbb{U}_n$ . Suppose further that  $x + (-2)^{\sigma-1} \in -(-2)^{\sigma-1} \langle x \rangle$ . Write  $S$  for the sequence*

$$+2^0 \ -2^0 \ -2^1 \ +2^1 \ +2^2 \ -2^2 \ \dots \ (-2)^{\sigma-1} \ -(-2)^{\sigma-1} \pmod n.$$

Then

$$\leftrightarrow x^0 S \mid x^1 S \mid \dots \mid x^{\pi-1} S \mid \leftrightarrow \pmod n$$

is a daisy chain for  $\mathbb{U}_n$ , where  $x^k S$  denotes the sequence  $S$  multiplied throughout by  $x^k$  ( $k = 0, 1, \dots, \pi - 1$ ).

**Proof:** Very similar to previous proofs. □

**Coverage of Theorem 5.1:** In the range  $1 < n < 300$  Theorem 5.1 covers the values  $n = pqr$  listed in the following table, which gives a specimen  $x$ -value for each; a double asterisk \*\* marks solutions with  $x^{-2} \equiv 4 \pmod{n}$ .

$n$	$\xi(n)$	$\pi$	$\sigma$	$x$
$105 = 3 \cdot 5 \cdot 7$	4	12	2	88**
$165 = 3 \cdot 5 \cdot 11$	4	20	2	28**
$195 = 3 \cdot 5 \cdot 13$	8	12	4	172
$231 = 3 \cdot 7 \cdot 11$	4	30	2	193**
$255 = 3 \cdot 5 \cdot 17$	8	16	4	22
$273 = 3 \cdot 7 \cdot 13$	12	12	6	85
$285 = 3 \cdot 5 \cdot 19$	4	36	2	13

In the range  $1 < n < 300$  Theorem 5.1 also covers the values  $n = p^i q^j$  ( $i \geq 1, j \geq 1$ ),  $\xi(n) > 4$ , that are listed in the following table; again a specimen  $x$ -value is given for each.

$n$	$\xi(n)$	$\pi$	$\sigma$	$x$	$n$	$\xi(n)$	$\pi$	$\sigma$	$x$
$63 = 3^2 \cdot 7$	6	6	3	19	$217 = 7 \cdot 31$	6	30	3	—
$91 = 7 \cdot 13$	6	12	3	6	$247 = 13 \cdot 19$	6	36	3	232
$117 = 3^2 \cdot 13$	6	12	3	31	$259 = 7 \cdot 37$	6	36	3	69
$133 = 7 \cdot 19$	6	18	3	61	$275 = 5^2 \cdot 11$	10	20	5	188
$171 = 3^2 \cdot 19$	6	18	3	154	$279 = 3^2 \cdot 31$	6	30	3	199
$189 = 3^3 \cdot 7$	6	18	3	166					

**Example 5.1(a):** For  $n = 105$  we have  $\pi = 12$  and  $\sigma = 2$ . If we take  $x$  in Theorem 5.1 to be the primitive  $\lambda$ -root 88 of 105, we have

$$x + (-2)^{\sigma-1} = 86 = 2x^9 \in -(-2)^{\sigma-1}\langle x \rangle .$$

Thus the value  $x = 88$  satisfies the conditions of Theorem 5.1, and we have the following daisy chain for  $\mathbb{U}_{105}$ :

$$\leftrightarrow 1 \ 104 \ 103 \ 2 \mid 88 \ 17 \ 34 \ 71 \mid 79 \ 26 \ 52 \ 53 \mid \dots \mid 37 \ 68 \ 31 \ 74 \mid \leftrightarrow .$$

**Example 5.1(b):** For  $n = 63 = 3^3 \cdot 7$  we have  $\pi = 6$  and  $\sigma = 3$ . We can take  $x = 19$  in Theorem 5.1 to obtain the following daisy chain for  $\mathbb{U}_{63}$ :

$$\begin{aligned} &\leftrightarrow 1 \ 62 \ 61 \ 2 \ 4 \ 59 \mid 19 \ 44 \ 25 \ 38 \ 13 \ 50 \mid 46 \ 17 \ 34 \ 29 \ 58 \ 5 \mid \\ &55 \ 8 \ 16 \ 47 \ 31 \ 32 \mid 37 \ 26 \ 52 \ 11 \ 22 \ 41 \mid 10 \ 53 \ 43 \ 20 \ 40 \ 23 \mid \leftrightarrow . \end{aligned}$$

In this example, we could alternatively have taken  $x = 34$  or  $x = 40$ .

If  $n = 3pq$  where  $p$  and  $q$  are distinct odd primes neither of which is 3, constructions for daisy chains for  $\mathbb{U}_{pq}$  can be modified to produce daisy chains for  $\mathbb{U}_n$ . To avoid notational complexities we omit details; we give the following single illustrative example.

**Example 5.2:** For  $pq = 65$  we can, as we have seen, take  $(z, x) = (34, 43)$  in Theorem 4.3 to obtain a daisy chain for  $\mathbb{U}_{65}$ . Suppose, however, that we now work modulo  $195 (= 3 \cdot 65 = n)$  and we take  $(z, x) = (164, 43)$ , the values of  $z = 34 + kx$  and  $x = 43 + \ell x$  (for some  $k$  and  $\ell$ ) being chosen so that none of  $z, z - 1$  and  $x$  is a multiple of 3. The chain given in the statement of Theorem 4.3, evaluated modulo 195, now contains exactly half of the units of  $\mathbb{Z}_{195}$ , the absent units being the negatives of those that are present. The differences for the chain likewise comprise exactly half of the units of  $\mathbb{Z}_{195}$ , the absent values again being the negatives of the units that are present. Now insert 2 extra elements after each of the first, third, fifth, ... elements of the chain to obtain the following:

$$\begin{aligned} &\hookrightarrow z^0 \quad -z^0 \quad -z^1 \quad z^1 \quad z^2 \quad -z^2 \quad -z^3 \quad z^3 \mid \\ &xz^0 \quad -xz^0 \quad -xz^1 \quad xz^1 \quad xz^2 \quad -xz^2 \quad -xz^3 \quad xz^3 \mid x^2z^0 \quad \dots \mid \dots \mid \hookleftarrow . \end{aligned}$$

This produces the following daisy chain for  $\mathbb{U}_{195}$ :

$$\begin{aligned} &\hookrightarrow 1 \quad 194 \quad 31 \quad 164 \quad 181 \quad 14 \quad 151 \quad 44 \mid \\ &\quad 43 \quad 152 \quad 163 \quad 32 \quad 178 \quad 17 \quad 58 \quad 137 \mid 94 \quad \dots \mid \dots \mid \hookleftarrow . \end{aligned}$$

The daisy chain is of the form

$$\hookrightarrow y^0 \quad cy^0 \quad y^1 \quad cy^1 \quad y^2 \quad cy^2 \quad y^3 \quad cy^3 \mid xy^0 \quad \dots \mid \dots \mid \hookleftarrow \pmod n$$

where  $y = -z$  and  $c = -1$ .

## 6 Fertility and green manures

We have seen in Theorem 2.1 that, if  $n$  is an odd prime power, then a daisy chain for  $\mathbb{U}_n$  is provided by the cycle of successive powers of a primitive root of  $n$ . The chain of differences  $b_i = a_{i+1} - a_i$  then itself consists of the successive powers of the self-same primitive root. But are there other circumstances in which the chain of differences is itself a daisy chain?

Let  $\chi_1$  be a daisy chain, and let  $\chi_2$  be the corresponding chain of differences. Let  $\chi_3$  be the chain of differences for  $\chi_2$ , and so on. If  $\chi_1, \chi_2, \dots, \chi_t$  are daisy chains but  $\chi_{t+1}$  is not, we say that  $\chi_1$  is *t-fertile*.

**Example 6.1:** For  $n = 21$ , consider the daisy chain of the form given in Note 3.1, namely

$$\begin{aligned} \chi_1 &= \hookrightarrow +1 \quad -1 \quad -2 \quad +2 \quad +4 \quad -4 \quad \dots \quad \hookleftarrow \\ &= \hookrightarrow 1 \quad 20 \quad 19 \quad 2 \quad 4 \quad 17 \quad 13 \quad 8 \quad 16 \quad 5 \quad 10 \quad 11 \quad \hookleftarrow . \end{aligned}$$



Here

$$\begin{aligned} \chi_2 &= \hookleftarrow 19\ 20\ 4\ 2\ 13\ 17\ 16\ 8\ 10\ 5\ 1\ 11 \hookleftarrow, \\ \chi_3 &= \hookleftarrow 1\ 5\ 19\ 11\ 4\ 20\ 13\ 2\ 16\ 17\ 10\ 8 \hookleftarrow, \\ \chi_4 &= \hookleftarrow 4\ 14\ 13\ 14\ 16\ 14\ 10\ 14\ 1\ 14\ 19\ 14 \hookleftarrow. \end{aligned}$$

Thus  $\chi_2$  is a daisy chain but  $\chi_3$  is not, so  $\chi_1$  is 2-fertile. Here  $\chi_3$  fails to be a daisy chain as alternate entries in  $\chi_4$  are equal to 14 (a multiple of a factor of  $n$ ).

**Example 6.2:** For  $n = 39$ , the daisy chain of the form given in Note 3.1 is

$$\hookleftarrow 1\ 38\ 37\ 2\ 4\ 35\ 31\ 8\ 16\ 23\ 7\ 32\ 25\ 14\ 28\ 11\ 22\ 17\ 34\ 5\ 10\ 29\ 19\ 20 \hookleftarrow,$$

which is 5-fertile. If we take this daisy chain to be  $\chi_1$ , the corresponding chain  $\chi_6$  fails to be a daisy chain as alternate entries in  $\chi_7$  are equal to 13 (a factor of  $n$ ).

As can be seen in the last two examples, the first two elements of  $\chi_3$  are 1 and 5 when the construction from Note 3.1 is used for  $\chi_1$ . If that construction is used when  $n$  is a suitable prime satisfying  $n \equiv 3 \pmod{8}$ , then both of the elements 1 and 5 are quadratic residues if and only if  $n \equiv \pm 1 \pmod{10}$ . Thus the construction merely produces a 1-fertile daisy chain if  $n = 11, 19$  or  $59$ . However, it produces a 2-fertile daisy chain for  $n = 67$  and a 3-fertile daisy chain for  $n = 83$ .

No detailed study of  $t$ -fertility in daisy chains has been made. But there is another interesting aspect to the sequence  $\chi_1, \chi_2, \dots$ . In discussing this, we regard two daisy chains  $\mathbf{a}$  and  $\mathbf{\alpha}$  as being *the same* if, for some  $c$ , we have  $a_i = \alpha_{i+c}$  ( $\forall i \in \{1, 2, \dots, \phi(n)\}$ ) where  $\alpha_{\phi(n)+1} = \alpha_1, \alpha_{\phi(n)+2} = \alpha_2, \text{ etc.}$

If  $\chi_1$  is  $t$ -fertile, then  $\chi_{t+1}$  must fail to be a daisy chain as a result of  $\chi_{t+2}$  not comprising each unit exactly once. So  $\chi_{t+2}$  is not a daisy chain either. However,  $\chi_{t+3}$  may then be a daisy chain. Indeed, it might be the same as  $\chi_1$ , or it might be the negative of  $\chi_1$ , or it might be a different daisy chain from either  $\chi_1$  or  $-\chi_1$ . If  $\chi_{t+3}$  is the negative of  $\chi_1$ , then  $\chi_{2t+5}$  will be the same as  $\chi_1$ .

If, in general,  $s$  is the smallest positive integer such that  $\chi_{s+1}$  is the same as  $\chi_1$  (or the same as a translate of  $\chi_1$ , see below), the succession of chains  $\chi_1, \chi_2, \dots, \chi_s$  is analogous to the succession of crops in the  $s$  years (or seasons) of an  $s$ -course rotation of crops in agriculture [17]. Accordingly we then say that  $\chi_1, \chi_2, \dots, \chi_s$  yield an  $s$ -course rotation of chains. We have required  $\chi_1$  to be a daisy chain but, as we have seen, two or more of the  $s$  courses may not contain daisy chains. These courses are analogous to agricultural rotation-courses where the crop is not harvested but is ploughed in for future benefit; such crops are used as ‘green manures’, and we analogously refer to *green-manure* courses or chains in our  $s$ -course rotations of chains.

**Example 6.1 (cont.):** Here,  $\chi_5$  is the negative of  $\chi_1$ , and so  $\chi_9$  is the same as  $\chi_1$ . We thus have an 8-course rotation containing 4 daisy chains ( $\chi_1, \chi_2, \chi_5$  and  $\chi_6$ ) and 4 green-manure chains ( $\chi_3, \chi_4, \chi_7$  and  $\chi_8$ ).

**Example 6.2 (cont.):** Here,  $\chi_8$  is the same as  $\chi_1$ , so we have a 7-course rotation containing 5 daisy chains and 2 green-manure chains.

**Example 6.3:** For  $n = 35$ , consider the daisy chain

$$\begin{aligned} \chi_1 &= \leftarrow +1 \ -1 \ -2 \ +2 \ +4 \ -4 \ -8 \ \dots \ \leftarrow \\ &= \leftarrow \ 1 \ 34 \ 33 \ 2 \ 4 \ 31 \ 27 \ \dots \ \leftarrow . \end{aligned}$$

This is 1-fertile. In the sequence  $\chi_1, \chi_2, \dots$ , the next daisy chains are  $\chi_{10}$  and  $\chi_{25}$ , this latter being the negative of  $\chi_1$ . We thus have a 48-course rotation containing just 4 daisy chains ( $\chi_1, \chi_{10}, \chi_{25}, \chi_{34}$ ) amidst 44 green-manure chains. (This is not practical agriculture!)

As we indicated above, we can have an  $s$ -course rotation where  $\chi_{s+1}$  is not the same as  $\chi_1$  but is the same as a translate of  $\chi_1$ . This situation is achievable when  $n = p^i$  ( $i > 1$ ) for some odd prime  $p$ , as a daisy chain for such a value of  $n$  remains a daisy chain when some constant multiple of  $p$  is added to all its elements.

**Example 6.4:** For  $n = 25$  consider the following daisy chain  $\chi_1$ :

$$1 \ 18 \ 14 \ 7 \ 16 \ 13 \ 24 \ 12 \ 6 \ 8 \ 9 \ 17 \ 21 \ 3 \ 19 \ 22 \ 11 \ 23 \ 4 \ 2 .$$

This is an  $\infty$ -fertile daisy chain, for which  $\chi_5$  is the daisy chain given in Ex. 2.2(c). Clearly  $\chi_1$  is obtained by adding 5 to  $\chi_5$  throughout. This example gives us a 4-course rotation with no green-manure courses.

## 7 The link between daisy chains and terraces

We now briefly present two results that show how daisy chains can be used in the construction of terraces.

Let  $\mathbf{a}$  be a **linear** arrangement  $(a_1, a_2, \dots, a_n)$  of **all** the elements of  $\mathbb{Z}_n$ , and let  $\mathbf{b}$  be the sequence  $(b_1, b_2, \dots, b_{n-1})$  given by  $b_i = a_{i+1} - a_i$  ( $i = 1, 2, \dots, n - 1$ ). Then [5]  $\mathbf{a}$  is a *terrace* for  $\mathbb{Z}_n$  (in short, a  $\mathbb{Z}_n$  terrace) if the sequences  $\mathbf{b}$  and  $-\mathbf{b}$  together contain exactly 2 occurrences of each element from  $\mathbb{Z}_n \setminus \{0\}$ . (A terrace for  $\mathbb{Z}_n$  provides a partition of the edges of  $2K_n$  into Hamiltonian paths, invariant under a group acting regularly.) When we present a terrace in a display, we omit brackets and commas.

**Result 7.1** *Suppose that  $[a_1, a_2, \dots, a_{n-1}]$  is a daisy chain for the units of  $\mathbb{Z}_n$  for some odd prime  $n$ . If  $a_{i+1} \equiv 2a_i \pmod{n}$  for some  $i$ , then*

$$a_{i+1} \ a_{i+2} \ \dots \ a_{n-1} \ a_1 \ a_2 \ \dots \ a_i \ | \ 0$$

*is a terrace for  $\mathbb{Z}_n$ . Likewise, if  $2a_{i+1} \equiv a_i \pmod{n}$  for some  $i$ , then*

$$0 \ | \ a_{i+1} \ a_{i+2} \ \dots \ a_{n-1} \ a_1 \ a_2 \ \dots \ a_i$$

*is a terrace for  $\mathbb{Z}_n$ .*

**Example 7.1:** The daisy chain

$$\leftrightarrow 1 \ 2 \ 5 \ 4 \ 6 \ 3 \ \leftarrow \pmod 7$$

for the units of  $\mathbb{Z}_7$  has  $x_2 = 2x_1$  and  $2x_6 = x_5$ . It thus yields the  $\mathbb{Z}_7$  terraces

$$2 \ 5 \ 4 \ 6 \ 3 \ 1 \mid 0$$

and

$$0 \mid 3 \ 1 \ 2 \ 5 \ 4 \ 6.$$

**Result 7.2** *Let  $n = p^2$  where  $p$  is an odd prime. Suppose that the cycle  $\mathbf{a} = [a_1, a_2, \dots, a_{p(p-1)}]$  is a daisy chain for the units of  $\mathbb{Z}_n$  and that the cycle  $\alpha = [\alpha_1, \alpha_2, \dots, \alpha_{p-1}]$  is a daisy chain for the units of  $\mathbb{Z}_p$ . If  $a_{i+1} \equiv 2a_i \pmod n$  for some  $i$ , and  $2\alpha_{j+1} = \alpha_j \pmod p$  for some  $j$ , then*

$$\begin{array}{cccccccccc}
 a_{i+1} & a_{i+2} & \dots & a_{p(p-1)} & a_1 & \dots & a_i & \mid & 0 & \mid \\
 p\alpha_{j+1} & p\alpha_{j+2} & \dots & p\alpha_{p-1} & p\alpha_1 & \dots & p\alpha_j & & & 
 \end{array}$$

is a terrace for  $\mathbb{Z}_n$ .

**Example 7.2:** Take  $n = p^2 = 11^2 = 121$ . Then  $\mathbf{a} = [1, 2, 4, \dots, 2^{109}]$  is a daisy chain for the units of  $\mathbb{Z}_n$ , and  $\alpha = [1, 2, 4, 9, 6, 10, 5, 8, 7, 3]$  is a daisy chain for the units of  $\mathbb{Z}_p$  (see §1). As  $2\alpha_8 = 2 \cdot 8 = 16 \equiv 5 = \alpha_7 \pmod{11}$ , we can take  $i = 110$  and  $j = 7$  in Result 7.2 to obtain the  $\mathbb{Z}_{121}$  terrace

$$\underbrace{1 \ 2 \ 4 \ \dots \ 61}_{110 \text{ terms}} \mid 0 \mid 88 \ 77 \ 33 \ 11 \ 22 \ 44 \ 99 \ 66 \ 110 \ 55.$$

**Acknowledgments**

The author is very grateful to M. A. Ollis (Marlboro College), R. A. Bailey (Queen Mary, University of London), M. J. Grannell (Open University) and a referee for helpful input.

**References**

- [1] I. Anderson and D. A. Preece, Power-sequence terraces for  $\mathbb{Z}_n$  where  $n$  is an odd prime power, *Discrete Math.* **261** (2003), 31–58.
- [2] I. Anderson and D. A. Preece, Narcissistic half-and-half power-sequence terraces for  $\mathbb{Z}_n$  with  $n = pq^t$ , *Discrete Math.* **279** (2004), 33–60.
- [3] I. Anderson and D. A. Preece, A general approach to constructing power-sequence terraces for  $\mathbb{Z}_n$ , *Discrete Math.*, to appear.
- [4] J.-M. Azais, Design of experiments for studying intergenotypic competition, *J. Royal Statist. Soc. B* **49** (1987), 334–345.

- [5] R. A. Bailey, Quasi-complete Latin squares: construction and randomisation, *J. Royal Statist. Soc. B* **46** (1984), 323–334.
- [6] G. K. Bennett, M. J. Grannell and T. S. Griggs, Cyclic bi-embeddings of Steiner triple systems on  $12s + 7$  points, *J. Combin. Designs* **10** (2002), 92–110.
- [7] P. J. Cameron and D. A. Preece, *Notes on Primitive  $\lambda$ -roots*, <http://www.maths.qmul.ac.uk/~pjc/cgsnotes/lambda.pdf> .
- [8] R. D. Carmichael, Note on a new number theory function, *Bull. Amer. Math. Soc.* **16** (1909–10), 232–237.
- [9] R. D. Carmichael, Generalizations of Euler’s  $\phi$ -function, with applications to Abelian groups, *Quart. J. Math.* **44** (1913), 94–104.
- [10] H. Dacre, *Daisy Bell*, T. B. Harms, New York, 1892.
- [11] R. J. Friedlander, B. Gordon and M. D. Miller, On a group sequencing problem of Ringel, *Congressus Numerantium* **21** (1978), 307–321.
- [12] M. J. Grannell, T. S. Griggs and J. Širáň, Surface embeddings of Steiner triple systems, *J. Combin. Designs* **6** (1998), 325–336.
- [13] P. Headley, R-sequenceability and  $R^*$ -sequenceability of abelian 2-groups, *Discrete Math.* **131** (1994), 345–350.
- [14] G. A. Jones and J. M. Jones, *Elementary Number Theory*, Springer, London, 1998.
- [15] M. A. Ollis, On terraces for abelian groups, *Discrete Math.* **305** (2005), 250–263.
- [16] L. J. Paige, Complete mappings of finite groups, *Pacific J. Math.* **1** (1951), 111–116.
- [17] D. A. Preece, Some general principles of crop rotation experiments, *Experimental Agriculture* **22** (1986), 187–198.
- [18] G. Ringel, *Map Color Theorem*, Springer, Berlin, 1974.
- [19] J. W. T. Youngs, The mystery of the Heawood conjecture, in: *Graph Theory and its Applications* (ed. B. Harris), pp. 17–50, Academic Press, New York, 1970.

(Received 21 July 2007)