AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **45** (2009), Pages 157–174

Daisy chains with three generators

D. A. Preece

Queen Mary University of London
School of Mathematical Sciences
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

For many positive odd integers n, whether prime, prime power or composite, the set $\mathbb{U}_n$ of units of $\mathbb{Z}_n$ contains members u, v and w, say with respective orders ψ, ω and π, such that we can write $\mathbb{U}_n$ as the direct product $\mathbb{U}_n = \langle u\rangle \times \langle v\rangle \times \langle w\rangle$. Each element of $\mathbb{U}_n$ can then be written in the form $u^i v^j w^k$ where $0 \le i \le \psi - 1$, $0 \le j \le \omega - 1$ and $0 \le k \le \pi - 1$. We can then often use the structure of $\langle u\rangle \times \langle v\rangle \times \langle w\rangle$ to arrange the $\psi\omega\pi$ elements of $\mathbb{U}_n$ in a *daisy chain*, *i.e.* in a circular arrangement such that, as we proceed round the chain in either direction, the set of differences between each member and the preceding one is itself the set $\mathbb{U}_n$. We describe such daisy chains as *daisy chains with three generators*. Each such daisy chain consists of a succession of *super-segments* of length $\omega\pi$, each made of *segments* of length π. Within each segment, each successive element is obtained from the preceding one by multiplication by w; within each super-segment, each successive segment is obtained from the preceding one by multiplication by v; each successive super-segment is obtained from the preceding one by multiplication by u. We study the existence of such arrangements, some of which can be obtained from general constructions which we describe. In many of our examples of the arrangements, one of the generators has order 2; if n is prime, that generator must then be $-1 \pmod n$, but if n is composite, another square root of $1 \pmod n$ may occasionally be used.

1 Introduction

Any positive integer n has a *prime-power decomposition*

$$n = p^i q^j r^k \cdots \quad (i, j, k \geq 1)$$

where $p, q, r, \ldots$ are finitely many distinct primes. In standard terminology, the *units* of the corresponding group $\mathbb{Z}_n$ 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*

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

(*e.g.* [4, p. 87]). For n odd, a *daisy chain* [5] for the units of $\mathbb{Z}_n$ (in short, a $\mathbb{Z}_n$ daisy chain) is an ordered arrangement $[a_1, a_2, \ldots, a_{\phi(n)}]$ of the units on a circle, such that the set of differences $b_i = a_{i+1} - a_i$ $(i = 1, 2, \ldots, \phi(n)$, with $a_{\phi(n)+1} = a_1)$ is itself the set of units. Here, as in [5] and elsewhere, we use square brackets to indicate a cycle. However, also as in [5], we replace [and] by $\hookrightarrow$ and $\hookleftarrow$ when we present a specific daisy chain in a display, and we then replace the commas by spaces. We henceforth use 'difference' to mean a right-minus-left difference of the above form $a_{i+1} - a_i$.

Various systematic methods of construction of daisy chains for $\mathbb{Z}_n$ were given in [5], where the emphasis was on values of n lying in the range $1 < n < 300$. We now investigate a new type of construction, which proves to be fruitful for both prime and composite values of n. To give a reasonable illustration of the scope of this new type, we now need to extend upwards the range of values of n.

For many positive odd integers n, whether prime, prime power or composite, the set $\mathbb{U}_n$ of units of $\mathbb{Z}_n$ contains members u, v and w, say with respective orders ψ, ω and π, such that we can write $\mathbb{U}_n = \langle u \rangle \times \langle v \rangle \times \langle w \rangle$. (Here, as subsequently in this paper, the symbol $\times$ indicates a direct product.) All, some or none of the orders ψ, ω and π may be prime. Each element of $\mathbb{U}_n$ can then be written in the form $u^i v^j w^k$ where $0 \leq i \leq \psi - 1$, $0 \leq j \leq \omega - 1$ and $0 \leq k \leq \pi - 1$. We can then often use the structure of $\langle u \rangle \times \langle v \rangle \times \langle w \rangle$ to arrange the $\psi\omega\pi$ elements of $\mathbb{U}_n$ in a daisy chain for $\mathbb{Z}_n$. We describe such daisy chains as *daisy chains with three generators*. Each such daisy chain consists of a succession of *super-segments* of length $\omega\pi$, each made up of *segments* of length π. Within each segment, each successive element is obtained from the preceding one by multiplication by w; within each super-segment, each successive segment is obtained from the preceding one by multiplication by v; each successive super-segment is obtained from the preceding one by multiplication by u. Thus, a daisy chain with three generators is of the following form where, as in [5], a *single fence* | denotes a boundary between two segments within a supersegment, and a *double fence* ‖ denotes a boundary between supersegments:

$$
\begin{array}{lccccc}
\hookrightarrow & u^0v^0w^0 & u^0v^0w^1 & \dots & u^0v^0w^{\pi-1} & | \\
& u^0v^1w^0 & u^0v^1w^1 & \dots & u^0v^1w^{\pi-1} & | \\
& & \vdots & & & \\
& u^0v^{\omega-1}w^0 & u^0v^{\omega-1}w^1 & \dots & u^0v^{\omega-1}w^{\pi-1} & \| \\
& & & & & \\
& u^1v^0w^0 & u^1v^0w^1 & \dots & u^1v^0w^{\pi-1} & | \\
& u^1v^1w^0 & u^1v^1w^1 & \dots & u^1v^1w^{\pi-1} & | \\
& & \vdots & & & \\
& u^1v^{\omega-1}w^0 & u^1v^{\omega-1}w^1 & \dots & u^1v^{\omega-1}w^{\pi-1} & \| \\
& \vdots & & & & \\
& u^{\psi-1}v^0w^0 & u^{\psi-1}v^0w^1 & \dots & u^{\psi-1}v^0w^{\pi-1} & | \\
& u^{\psi-1}v^1w^0 & u^{\psi-1}v^1w^1 & \dots & u^{\psi-1}v^1w^{\pi-1} & | \\
& & \vdots & & & \\
& u^{\psi-1}v^{\omega-1}w^0 & u^{\psi-1}v^{\omega-1}w^1 & \dots & u^{\psi-1}v^{\omega-1}w^{\pi-1} & \| \quad \hookleftarrow
\end{array}
$$

As a daisy chain may be read anticlockwise as well as clockwise, the existence of a particular daisy chain with the three generators u, v and w implies the existence of a daisy chain with the three generators u^{-1}, v^{-1} and w^{-1}. For this reason, the distinct parameter sets (u, v, w) for any particular n arise in pairs; we use N_n to denote the number of such pairs.

For prime values of n in the range $n < 400$, Table 1 below gives parameter sets (ψ, ω, π) and (u, v, w) for $\mathbb{Z}_n$ daisy chains with three generators. Table 2 similarly covers prime powers $n = p^j$ $(j > 1)$, whereas Table 3 covers composite values of n in the range $n < 140$. For each n in Table 3, we use $\xi(n)$, as in [1], to denote the value of $\phi(n)/\lambda(n)$ where $\lambda(n)$, which is Carmichael's λ-function [2, 3], gives the order of an element of maximum order in $\mathbb{U}_n$. (If n is odd and composite, then $\xi(n)$ is even [1].)

Longer versions of Tables 1 and 3 can be viewed [6] via the *Australasian Journal of Combinatorics* website. There, Table 1 is for $n < 500$, and the much longer Table 3 is for $n < 350$.

As indicated by the footnotes to Tables 1 and 3, many of the parameter sets (u, v, w) satisfy simple relationships such as $u + 2v \equiv 0 \pmod{n}$ or $(u + 1)vw \equiv 1 \pmod{n}$. Mostly, we give only one parameter set (u, v, w) for any particular set (ψ, ω, π) for any particular value of n, but we give two or more sets (u, v, w) if each of the listed possibilities satisfies one of the listed simple relationships. Some of these relationships arise from general constructions that can be formalised and proved, as in Sections 2 and 3 below; others arise unexplained.

The relationship $(u + 1)vw \equiv 1 \pmod{n}$, satisfied by many examples in Tables 1 and 3, requires the first element of the second supersegment to be 1 less than the final element of the first supersegment. This situation reflects that of Theorems 2.3 and 4.1 of [5], where the first element of the second segment of a daisy chain is 1 less than the final element of the first segment. However, the relationship $(u - 1)vw \equiv 1 \pmod{n}$ also arises for various primes, *e.g.* $n = 379$, 431, 457 and 491 (Table 1); then the first element of the second supersegment is 1 **more** than the final element of the first supersegment.

For composite values of n, the relationships $u(v+1)w \equiv 1 \pmod{n}$ and $(u^2+1)vw \equiv 1 \pmod{n}$ frequently occur too. The latter is often satisfied simultaneously with $u^2 \equiv 2vw \pmod{n}$, in which case we have $(u^2-1)(u^2+2) \equiv 0 \pmod{n}$ and $(2vw-1)(vw+1) \equiv 0 \pmod{n}$.

Note 1.1: In many of our examples of daisy chains with three generators, one of the generators has order 2. If n is prime, that generator must then be $-1 \pmod{n}$, but if n is composite, another square root of 1 (mod n) may perhaps be used; we obtain examples of this for $n = 63$, 91, 133, 171, 189, 213, 217, 247, 259, 275, 279, 301, 309, 315, 335 and 341 (see Table 3).

Note 1.2: Constructions for $\mathbb{Z}_n$ daisy chains with two generators were given in [5], but at least three generators are needed if analogous constructions are to be provided for odd composite integers n that have three distinct odd prime factors. For n-values of this last type, we now provide three-generator daisy chains for $n = 105$, 165, 195, 231, 255, 273, 315 and 345 (again see Table 3).

Note 1.3: A special type of daisy chain for $\mathbb{Z}_n$ has the property that

$$a_i \equiv -a_{i+\phi(n)/2} \pmod{n}$$

for $i = 1, 2, \ldots, \phi(n)/2$. For $\mathbb{Z}_n$ daisy chains with 3 generators, this property is achieved if ψ is even, with $u^{\psi/2} \equiv -1 \pmod{n}$. We obtain examples of this for $n = 241$, 331, 337, 409, 421, and 463 (prime, Table 1), for $n = 169 = 13^2$ (Table 2) and for $n = 145$ and 259 (composite, Table 3). Having ψ even is not a sufficient condition for the property.

2 Some theorems, n prime

We now provide eight theorems that embody general constructions for $\mathbb{Z}_n$ daisy chains with three generators. Theorems 2.1–2.3 are for prime values of n, and Theorems 3.1–3.5 are for composite values.

Theorem 2.1 *Let n be a prime such that $n \equiv 43$ or $67 \pmod{72}$. Let y be an element of order 3 in $\mathbb{Z}_n$, and suppose that there exists an element x, of order $(n-1)/6$ in $\mathbb{Z}_n$, such that*

$$x - y - 1 \equiv -x^i y \pmod{n}$$

for some i from $\{2, 3, \ldots, (n-1)/6\}$. Then, for $\mathbb{Z}_n$, there is a daisy chain with $(\psi, \omega, \pi) = ((n-1)/6,\ 3,\ 2)$ and parameters $(u, v, w) = (x,\ y,\ -1)$.

Proof: The conditions of the Theorem ensure that ψ, ω and π are mutually prime and that the product $\langle u \rangle \times \langle v \rangle \times \langle w \rangle$ is direct. As $n \equiv 1 \pmod{6}$, the element -3 is a quadratic residue modulo n, and as $y^2 + y + 1 \equiv 0 \pmod{n}$ we have $y \equiv 2^{-1}(-1 \pm \sqrt{-3}) \pmod{n}$. The proposed daisy chain is of the form

$$\hookrightarrow \quad 1 \quad -1 \quad | \quad y \quad -y \quad | \quad -(y+1) \quad y+1 \quad \| \quad x \quad \ldots \quad \hookleftarrow$$

where the first element in each segment is a quadratic residue modulo n, and the second is a quadratic non-residue. The difference in the first segment is -2, which is a quadratic residue, so the set of all the within-segment differences is precisely the set of quadratic residues. The difference at the first single fence is $y+1$, and that at the second single fence is -1, and these quadratic non-residues are respectively the sixth and second elements of the first super-segment. So we require the difference $x-y-1$ at the first double fence to equal the fourth element in one of the super-segments. The result follows. □

Note 2.1: Theorem 2.1 fails to yield a daisy chain for $n = 43$, but succeeds for $n = 67$, 139, 211, 283, and 331 (see Table 1) and for $n = 499$, 547, 571, 618, 643, 691, 787, 859 and 907.

Example 2.1: $n = 67$. With $y = 29$ we may, for example, take $x = 9$ in Theorem 2.1, as we then have

$$x - y - 1 \equiv 46 \equiv -x^7 y \pmod{n} .$$

This gives the following $\mathbb{Z}_{67}$ daisy chain (see Table 1), where the value $x - y - 1 \pmod{n}$ is marked with an asterisk:

		w		v					
		↓		↓					
↪	1	66	|	29	38	|	37	30	‖
$u \rightarrow$	9	58	|	60	7	|	65	2	‖
	14	53	|	4	63	|	49	18	‖
	59	8	|	36	31	|	39	28	‖
	62	5	|	56	11	|	16	51	‖
	22	45	|	35	32	|	10	57	‖
	64	3	|	47	20	|	23	44	‖
	40	27	|	21	46*	|	6	61	‖
	25	42	|	55	12	|	54	13	‖
	24	43	|	26	41	|	17	50	‖
	15	52	|	33	34	|	19	48	‖ ↩

Theorem 2.2 *Let n be a prime with $n \equiv 7 \pmod 8$. Suppose that $\mathbb{Z}_n \setminus \{0\}$ contains an element x such that the quadratic residues modulo n are the elements of $\langle x \rangle \times \langle x+1 \rangle$, with $2x+1 \in \langle x+1 \rangle$. Then, for $\mathbb{Z}_n$, there is a daisy chain with $(\psi, \omega, \pi) = (\mathrm{ord}_n(x+1),\ \mathrm{ord}_n(x),\ 2)$ and $(u, v, w) = (x+1,\ x^{-1},\ -1)$.*

Proof: The product $\langle u \rangle \times \langle v \rangle \times \langle w \rangle$ is direct as -1 is not a square in $\mathbb{Z}_n$. The proposed daisy chain is of the form

$$
\begin{array}{llllllllll}
\hookrightarrow & & & & & & & & & \\
1 & -1 & | & x^{-1} & -x^{-1} & | & & & & \\
 & & & x^{-2} & -x^{-2} & | & \dots & & & \\
 & & & & & | & x & -x & \| & \\
 & & & & & & & & & \\
x+1 & -(x+1) & | & x^{-1}+1 & -(x^{-1}+1) & | & & & & \\
 & & & x^{-1}(x^{-1}+1) & -x^{-1}(x^{-1}+1) & | & \dots & & & \\
 & & & & & | & x(x+1) & -x(x+1) & \| & \\
 & & & & & & & & & \\
(x+1)^2 & \dots & & & & & & & & \\
\vdots & & & & & & & & & \\
 & & & & & & & & & \hookleftarrow
\end{array}
$$

where the first element in each segment is a quadratic residue modulo n, and the second is a quadratic non-residue. The difference in the first segment is -2, which is a quadratic non-residue, so all the within-segment differences are quadratic non-residues. The differences at the 1^{st}, 2^{nd}, $\dots$, $(\omega-1)^{\text{th}}$ single fences are $x^{-1}+1$, $x^{-1}(x^{-1}+1)$, $x^{-2}(x^{-1}+1)$, $\dots$, namely the initial elements of the 2^{nd}, 3^{rd}, $\dots$, ω^{th} segments of the second supersegment. So we require the difference $2x+1$ at the first double fence to be the initial element of a supersegment. The results follows. □

Note 2.2: The smallest prime for which Theorem 2.2 yields a daisy chain is $n = 311$, with $x = 6 = 52^{-1}$ where $\operatorname{ord}_n(x) = 5$ and $\operatorname{ord}_n(x+1) = 31$ (see again Table 1).

Theorem 2.3 *Let n be a prime with $n \equiv 3 \pmod 8$. Suppose that $\mathbb{Z}_n \setminus \{0\}$ contains an element x, satisfying $1 < x < n-2$, such that*

$$\mathbb{Z}_n \setminus \{0\} = \langle x \rangle \times \langle x+1 \rangle = \langle y \rangle \times \langle y+1 \rangle$$

where $y \equiv -(x+1) \pmod n$, and where $\operatorname{ord}_n(x+1)$ and $\operatorname{ord}_n(y+1)$ are both even. Then there is a $\mathbb{Z}_n$ daisy chain (i) *with*

$$(\psi, \omega, \pi) = (\operatorname{ord}_n(x), \operatorname{ord}_n(y), 2), \qquad (u, v, w) = (x, y^{-1}, -1)\ ;$$

likewise there is a $\mathbb{Z}_n$ daisy chain (ii) *with*

$$(\psi, \omega, \pi) = (\operatorname{ord}_n(y), \operatorname{ord}_n(x), 2), \qquad (u, v, w) = (y, x^{-1}, -1)\ .$$

In each case we have $(u+1)vw \equiv 1 \pmod n$.

Proof: The proposed daisy chain (i) is of the form

$$
\begin{array}{llllllllllllll}
\hookrightarrow & 1 & -1 & | & y^{-1} & -y^{-1} & | & y^{-2} & -y^{-2} & | & \dots & | & y & -y & \| \\
 & x & -x & | & xy^{-1} & -xy^{-1} & | & xy^{-2} & -xy^{-2} & | & \dots & | & xy & -xy & \| \\
 & x^2 & \text{etc.} & & & & & & & & & & & & \\
 & \vdots & & & & & & & & & & & & & \hookleftarrow
\end{array}
$$

where the first element in each segment is a quadratic residue modulo n, and the second is not. The difference in the first segment is -2, which is a quadratic residue, so all the within-segment differences are quadratic residues. The differences at the 1^{st}, 2^{nd}, ..., $(\omega-1)^{th}$ single fences are $y^{-1}(1+y)$, $y^{-2}(1+y)$, ..., namely the second elements of the 2^{nd}, 3^{rd}, ..., ω^{th} segments of the second supersegment. The difference at the first double fence is $x+y=-1$, which is the second element of the 1^{st} segment of the first supersegment. The required result for (i) follows. □

Note 2.3: The smallest prime for which Theorem 2.3 yields daisy chains is $n = 331$ (see Table 1), for which we can take $x = 74$ where $\mathrm{ord}_n(x) = 11$ and $\mathrm{ord}_n(x+1) = 30$, with $y = 256$ where $\mathrm{ord}_n(y) = 15$ and $\mathrm{ord}_n(y+1) = 22$. With $n < 1000$, Theorem 2.3 yields daisy chains for $n = 331$, 443, 523, 547, 571, 659, 739, 827, 859 and 971.

3 Some theorems, n composite

We now turn to our theorems for odd composite values of n. Theorems 3.1, 3.2 and 3.3, like Theorem 2.1, provide daisy chains with $(\omega, \pi) = (3, 2)$.

Theorem 3.1 *Let n be a composite odd integer such that 6 divides $|\mathbb{U}_n|$. Suppose that $\mathbb{U}_n$ contains elements x and y, with $\mathrm{ord}_n(x) = |\mathbb{U}_n|/6$ and $\mathrm{ord}_n(y) = 3$, such that $y + y^2 \equiv -1 \pmod n$ and*

$$\mathbb{U}_n = \langle x \rangle \times \langle y \rangle \times \langle -1 \rangle \ .$$

Suppose further that $-2 \in \langle x \rangle \times \langle y \rangle$, and that

$$x - y - 1 \equiv -x^i y \pmod n$$

for some i from $\{2, 3, \ldots, \mathrm{ord}_n(x)\}$. Then there is a $\mathbb{Z}_n$ daisy chain with $(\psi, \omega, \pi) = (|\mathbb{U}_n|/6,\ 3,\ 2)$ and parameters $(u, v, w) = (x,\ y,\ -1)$.

Proof: If y is a unit of order 3 in $\mathbb{Z}_n$ where n is composite, y does not necessarily satisfy the condition $y + y^2 \equiv -1 \pmod n$, so the appearance of this condition in the statement of the theorem is not a redundancy (see Theorems 3.2 and 3.3 below). With this condition imposed, the proof is as for Theorem 2.1, save that the set of quadratic residues is replaced by the set $\langle x \rangle \times \langle y \rangle$. □

Note 3.1: In the range $n < 350$, we can use Theorem 3.1 for $n = 91$, 93, 129, 183, 201, 237, 291 and 309 (see Table 3).

Example 3.1: $n = 91 = 7 \times 13$. With $y = 16$, we can take $x = 19$ in Theorem 3.1, as we then have

$$x - y - 1 \equiv 2 \equiv -x^3 y \pmod n \ .$$

This gives the following $\mathbb{Z}_{91}$ daisy chain (see Table 3), where the value $x - y - 1 \pmod n$ is marked with an asterisk:

TABLE 1
Parameters for daisy chains with 3 generators
n prime ($n < 400$)

n	N_n	ψ	ω	π	Notes	Theorem	u	v	w
67	6	11	3	2	a	2.1	9	29	−1
					b	2.1	64	29	−1
		11	2	3	–	–	9	−1	29
71	2	7	5	2	–	–	30	5	−1
		7	2	5	–	–	45	−1	57
131	1	13	2	5	–	–	52	−1	58
139	3	23	3	2	b	2.1	65	42	−1
151	5	25	2	3	–	–	148	−1	32
157	1	13	4	3	–	–	46	28	12
181	2	9	5	4	–	–	39	59	162
		9	4	5	–	–	39	162	59
191	2	19	5	2	–	–	32	39	−1
199	2	9	11	2	–	–	175	114	−1
211	8	35	3	2	a	2.1	183	14	−1
		7	10	3	–	–	148	104	196
		7	6	5	–	–	148	15	107
229	6	19	4	3	j	–	17	107	134
		19	3	4	j	–	17	134	107
239	1	17	7	2	–	–	40	44	−1
241	3	16	5	3	–	Note 1.3	115	87	15
		16	3	5	–	Note 1.3	197	225	205
		5	16	3	j	–	87	197	15
271	2	27	5	2	–	–	160	244	−1
283	6	47	3	2	–	2.1	38	238	−1
307	1	9	17	2	–	–	274	235	−1
311	4	31	5	2	–	2.2	7	52	−1
313	1	13	8	3	–	–	103	188	98

continued. . .

TABLE 1 (continued)

n	N_n	ψ	ω	π	Notes	Theorem	u	v	w
331	9	55	3	2	–	2.1	144	31	−1
		33	5	2	–	–	198	150	−1
		22	5	3	j	–	164	64	31
		15	11	2	j	2.3	256	85	−1
		11	15	2	j	2.3	74	203	−1
		11	10	3	j	–	74	207	31
		10	11	3	–	Note 1.3	267	85	299
		6	11	5	–	–	32	120	124
337	2	16	7	3	–	Note 1.3	30	79	128
		7	16	3	j	–	64	59	208
349	3	29	3	4	–	–	110	226	136
367	6	61	2	3	–	–	101	−1	83
373	1	4	31	3	j	–	269	144	284
379	4	27	2	7	i	–	294	−1	119
		7	27	2	–	–	195	121	−1
		7	2	27	–	–	195	−1	121

Notes (all the congruences being interpreted modulo n):
[a] $u + 2v \equiv 0$ [i] $(u-1)vw \equiv 1$
[b] $u^2 + 2v \equiv 0$ [j] $(u+1)vw \equiv 1$

TABLE 2
Parameters for daisy chains with 3 generators
n a prime power $n = p^j$ with $j > 1$ ($n < 400$)

n	N_n	ψ	ω	π	u	v	w	
121	11	11	5	2	111^i	27	−1	($i = 1, 2, \ldots, 9$ or 10)
		5	11	2	9	12	−1	
169	13	13	4	3	105^i	99	146	($i = 1, 2, \ldots, 11$ or 12)
		4	13	3	99	105	146	
361	19	19	9	2	115^i	28	−1	($i = 1, 2, \ldots, 17$ or 18)
		9	19	2	245	248	−1	

$$
\begin{array}{rrcccccccl}
 & & w & & v & & & & & \\
 & & \downarrow & & \downarrow & & & & & \\
\hookrightarrow & 1 & 90 & | & 16 & 75 & | & 74 & 17 & \| \\
u \rightarrow & 19 & 72 & | & 31 & 60 & | & 41 & 50 & \| \\
 & 88 & 3 & | & 43 & 48 & | & 51 & 40 & \| \\
 & 34 & 57 & | & 89 & 2^* & | & 59 & 32 & \| \\
 & \vdots & & & & & & & & \\
 & 24 & 67 & | & 20 & 71 & | & 47 & 44 & \| \quad \hookleftarrow
\end{array}
\Bigg\} \text{12 supersegments}
$$

Theorem 3.2 *Let $n = 9m$ where m is an odd integer. Let $y = 1 + 3m$ or $1 + 6m$, and suppose that $\mathbb{U}_n$ contains an element x such that* $\mathrm{ord}_n(x) = |\mathbb{U}_n|/6$ *and*

$$\mathbb{U}_n = \langle x \rangle \times \langle y \rangle \times \langle -1 \rangle \ .$$

Suppose further that $-2 \equiv x^j y^2 \pmod{n}$ *and*

$$x - y + 2 \equiv -x^i \pmod{n}$$

for some values i and j from $\{2, 3, \ldots, \mathrm{ord}_n(x)\}$. Then there is a $\mathbb{Z}_n$ daisy chain with $(\psi, \omega, \pi) = (|\mathbb{U}_n|/6,\ 3,\ 2)$ and parameters $(u, v, w) = (x,\ y,\ -1)$.

Proof: The relationships $\mathrm{ord}_n(y) = 3$ and $y + 1 \equiv 2y^2 \pmod{n}$ are easily checked. The proposed daisy chain is of the form

$$\hookrightarrow \quad 1 \quad -1 \ | \ y \quad -y \ | \ -(y-2) \quad y-2 \ \| \ x \quad \ldots \quad \hookleftarrow$$

where the first element in each segment comes from $\langle x \rangle \times \langle y \rangle$. The difference in the first segment is -2, which comes from $\langle x \rangle \times \langle y \rangle$, so the set of all the within-segment differences is precisely the set $\langle x \rangle \times \langle y \rangle$. The difference at the second single fence is $+2$, and that at the first single fence is $y+1 \equiv 2y^2$, and these are respectively the sixth and fourth elements of one of the supersegments. So we require the difference $x-y+2$ at the first double fence to equal the second element of one of the supersegments. The result follows. □

Note 3.2: In the range $n < 350$, we can use Theorem 3.2 for $n = 45$, 63, 99, 117, 153, 171, 207, 225, 261, 279 and 333.

Example 3.2 $n = 99 = 3^2 \times 11$. With $y = 67$, we can take $x = 19$, 28, 46 or 73 in Theorem 3.2. Taking $x = 19$ gives the following $\mathbb{Z}_{99}$ daisy chain (see Table 3), where the value $x - y + 2 \pmod{n}$ is marked with a dagger:

$$
\begin{array}{rrrcrrcrrcc}
 & & w & & v & & & & & & \\
 & & \downarrow & & \downarrow & & & & & & \\
\hookrightarrow & 1 & 98 & | & 67 & 32 & | & 34 & 65 & \| & \\
u \rightarrow & 19 & 80 & | & 85 & 14 & | & 52 & 47 & \| & \\
 & 64 & 35 & | & 31 & 68 & | & 97 & 2 & \| & \\
 & 28 & 71 & | & 94 & 5 & | & 61 & 38 & \| & \\
 & 37 & 62 & | & 4 & 95 & | & 70 & 29 & \| & \\
 & 10 & 89 & | & 76 & 23 & | & 43 & 56 & \| & \\
 & 91 & 8 & | & 58 & 41 & | & 25 & 74 & \| & \\
 & 46 & 53^{\dagger} & | & 13 & 86 & | & 79 & 20 & \| & \\
 & 82 & 17 & | & 49 & 50 & | & 16 & 83 & \| & \\
 & 73 & 26 & | & 40 & 59 & | & 7 & 92 & \| & \hookleftarrow
\end{array}
$$

Theorem 3.3 *Let $n = 9m$ where m is an odd integer. Let $y = 1 + 3m$ or $1 + 6m$, and suppose that* $\mathrm{ord}_n(-2) = |\mathbb{U}_n|/6$ *and*

$$\mathbb{U}_n = \langle -2 \rangle \times \langle y \rangle \times \langle -1 \rangle \ .$$

Then there is a $\mathbb{Z}_n$ daisy chain with $(\psi, \omega, \pi) = (|\mathbb{U}_n|/6,\ 3,\ 2)$ and parameters $(u, v, w) = (-2,\ y,\ -1)$.

Proof: The proposed daisy chain is of the form

$$
\begin{array}{rrrcrrcrrcc}
\hookrightarrow & 1 & -1 & | & y & -y & | & -(y-2) & (y-2) & \| & \\
 & -2 & 2 & | & -2y & 2y & | & 2(y-2) & -2(y-2) & \| & \\
 & 4 & -4 & | & 4y & -4y & | & -4(y-2) & 4(y-2) & \| & \\
 & \vdots & & & & & & & & & \\
 & & & & & & & & & & \hookleftarrow
\end{array}
\ .
$$

Clearly, the set of within-segment differences is precisely the set of first elements within segments. As

$$(y + 1) + 2(y - 2) \equiv 3y - 3 \equiv 0 \pmod{n}$$

we have $y + 1 \equiv -2(y - 2)$, so the difference at the first single fence equals the final element of the second supersegment. The difference at the second single fence is $+2$, which is the second element of the second supersegment. The difference at the first double fence is $-y$, which is the fourth element of the first supersegment. The required result follows. □

Note 3.3: In the range $n < 350$, we can use Theorem 3.3 for $n = 63$, 117 and 333 (see Table 3).

Example 3.3: $n = 63 = 3^2 \times 7$. Taking $y = 22$ in Theorem 3.3 gives the following $\mathbb{Z}_{63}$ daisy chain (see Table 3):

$$
\begin{array}{rrrcrrcrrc}
 & & & w & v & & & & & \\
 & & & \downarrow & \downarrow & & & & & \\
\hookrightarrow & & 1 & 62 & 22 & 41 & 43 & 20 & \| & \\
 & u \rightarrow & 61 & 2 & 19 & 44 & 40 & 23 & \| & \\
 & & 4 & 59 & 25 & 38 & 46 & 17 & \| & \\
 & & 55 & 8 & 13 & 50 & 34 & 29 & \| & \\
 & & 58 & 5 & 37 & 26 & 16 & 47 & \| & \\
 & & 31 & 32 & 52 & 11 & 10 & 53 & \| & \hookleftarrow
\end{array}
$$

Theorem 3.4 *Let n be an odd composite integer. Suppose that $\mathbb{U}_n$ contains an element x such that*

$$\mathbb{U}_n = \langle x \rangle \times \langle x+1 \rangle \times \langle -1 \rangle$$

and $x(x+1)+2 \equiv 0 \pmod{n}$. Then there are $\mathbb{Z}_n$ daisy chains with
(i) $(\psi, \omega, \pi) = (\mathrm{ord}_n(x),\ \mathrm{ord}_n(x+1),\ 2)$ *and* $(u, v, w) = (x,\ x+1,\ -1)$,
and
(ii) $(\psi, \omega, \pi) = (\mathrm{ord}_n(x),\ 2,\ \mathrm{ord}_n(x+1))$ *and* $(u, v, w) = (x^{-1},\ -1,\ (x+1)^{-1})$.

Proof: The proposed daisy chain (i) is of the form

$$
\begin{array}{rrcrrcrrc}
\hookrightarrow 1 & -1 & | & (x+1) & -(x+1) & | & (x+1)^2 & -(x+1)^2 & | \\
 & & & & \ldots & | & (x+1)^{-1} & -(x+1)^{-1} & \| \\
x & -x & | & x(x+1) & -x(x+1) & | & x(x+1)^2 & -x(x+1)^2 & | \\
 & & & & \ldots & | & x(x+1)^{-1} & -x(x+1)^{-1} & \| \\
x^2 & -x^2 & | & x^2(x+1) & -x^2(x+1) & | & x^2(x+1)^2 & -x^2(x+1)^2 & | \\
 & & & & \ldots & | & x^2(x+1)^{-1} & -x^2(x+1)^{-1} & \| \\
\vdots & & & & & & & & \\
 & & & & & & & & \hookleftarrow
\end{array}
$$

The difference in the first segment is -2, which is the first entry in the second segment of the second supersegment. Thus the set of within-segment differences is precisely the set of first entries from each segment. The difference at the first single fence is $x+2 \equiv -x^2 \pmod{n}$, which is the second entry in the first segment of the third supersegment. Thus the set of differences at all the single fences is obtained by taking the second entry from every segment except a segment immediately preceding a double fence. Finally, the difference at the first double fence is

$$x + (x+1)^{-1} = (x+1)^{-1}[x(x+1)+1] \equiv -(x+1)^{-1} \pmod{n}\ ,$$

which is the final element of the first supersegment. The required result follows.

The proposed daisy chain (ii) is of the form

$$
\begin{array}{lccccc|l}
\hookrightarrow & 1 & (x+1)^{-1} & (x+1)^{-2} & \dots & (x+1) & | \\
 & -1 & -(x+1)^{-1} & -(x+1)^{-2} & \dots & -(x+1) & \| \\
 & x^{-1} & x^{-1}(x+1)^{-1} & x^{-1}(x+1)^{-2} & \dots & x^{-1}(x+1) & | \\
 & -x^{-1} & -x^{-1}(x+1)^{-1} & -x^{-1}(x+1)^{-2} & \dots & -x^{-1}(x+1) & \| \\
 & \vdots & & & & & \\
 & x^2 & x^2(x+1)^{-1} & x^2(x+1)^{-2} & \dots & x^2(x+1) & | \\
 & -x^2 & -x^2(x+1)^{-1} & -x^2(x+1)^{-2} & \dots & -x^2(x+1) & \| \\
 & x & x(x+1)^{-1} & x(x+1)^{-2} & \dots & x(x+1) & | \\
 & -x & -x(x+1)^{-1} & -x(x+1)^{-2} & \dots & -x(x+1) & \| \quad \hookleftarrow .
\end{array}
$$

The differences within the first segment are the entries, except the first, in the final segment. The differences at the single fences are the first entries of the first segments in the supersegments. The differences at the double fences are the first entries of the second segments in the supersegments. The required result follows. □

Note 3.4: Theorem 3.4 can be used for $n = 259$ (see Table 3).

We now come to an important analogue of Theorem 2.3.

Theorem 3.5 *Let n be an odd composite integer such that $\mathbb{U}_n$ contains an element x with*

$$\mathbb{U}_n = \langle x \rangle \times \langle y \rangle \times \langle -1 \rangle$$

where $y \equiv -(x+1) \pmod{n}$. Suppose that $-2 \in \langle x \rangle \times \langle y \rangle$. Then (as in Theorem 2.3*) there is a $\mathbb{Z}_n$ daisy chain* (i) *with*

$$(\psi, \omega, \pi) = (\mathrm{ord}_n(x), \mathrm{ord}_n(y), 2), \qquad (u, v, w) = (x, y^{-1}, -1) \ ;$$

likewise there is a $\mathbb{Z}_n$ daisy chain (ii) *with*

$$(\psi, \omega, \pi) = (\mathrm{ord}_n(y), \mathrm{ord}_n(x), 2), \qquad (u, v, w) = (y, x^{-1}, -1) \ .$$

In each case we have $(u+1)vw \equiv 1 \pmod{n}$.

Proof: As for Theorem 2.3. □

Note 3.5: Table 3 includes cases from Theorem 3.5. Often, but not always, such cases have $uv^{-1}w \equiv 2$ and therefore $u + 2v \equiv 0 \pmod{n}$.

Example 3.5: $n = 63$. With $x = 43$ and $(u, v, w) = (x, y^{-1}, -1) = (43, 10, 62)$, Theorem 3.5 gives the following $\mathbb{Z}_{63}$ daisy chain:

$$
\begin{array}{lcccccccccccccc}
 & & w & & v & & & & & & & & & x+1 & \\
 & & \downarrow & & \downarrow & & & & & & & & & \downarrow & \\
\hookrightarrow & 1 & 62 & | & 10 & 53 & | & 37 & 26 & | & 55 & 8 & | & 46 & 17 & | & 19 & 44 & \| \\
u \rightarrow & 43 & 20 & | & 52 & 11 & | & 16 & 47 & | & 34 & 29 & | & 25 & 38 & | & 61 & 2 & \| \\
 & 22 & 41 & | & 31 & 32 & | & 58 & 5 & | & 13 & 50 & | & 4 & 59 & | & 40 & 23 & \| \hookleftarrow
\end{array}
$$

4 More results for composite n

As indicated by the Notes to Table 3, many of its $\mathbb{Z}_n$ daisy chains have simple relationships between their parameters u, v and w. Further theorems could be provided to account for the appearance of some of these relationships, but we judge these theorems to be of little interest and to be too numerous to justify their inclusion.

Of more interest is a type of relationship that can exist between the parameters for a $\mathbb{Z}_n$ daisy chain for which n is of the form p^iq (p prime, $i > 1$) and those for a $\mathbb{Z}_n$ daisy chain for $n = p^{i-1}q$. Thus, for example, we can take $(u, v, w) = (106, 82, -1)$ for $n = 135 = 3^3 \times 5$, and $(u, v, w) = (16, 37, -1)$ for $n = 45 = 3^2 \times 5$ (see Table 3); here the second set of parameters is obtained by reducing the first set modulo 45. Likewise we can take $(u, v, w) = (109, 55, 95)$ for $n = 189 = 3^3 \times 7$, and $(u, v, w,) = (46, 55, 32)$ for $n = 63 = 3^2 \times 7$ (again see Table 3). However, a set of parameters (u, v, w) for p^iq, when reduced modulo $p^{i-1}q$, does not in general give a valid set of parameters (u, v, w) for $p^{i-1}q$.

Note 4.1: The Notes to Table 3 also draw attention to special situations that can arise when ψ and ω are both multiples of 3 and $\pi = 2$. We can then sometimes have

(a) $$u^{\psi/3} + v + 1 \equiv 0 \pmod{n}$$

or

(b) $$u^{2\psi/3} + v + 1 \equiv 0 \pmod{n}$$

in conjunction with $uv \equiv -2$ and $w \equiv -1 \pmod{n}$. At least one of these situations arises for each of $n = 63$, 117, 133, 247, 273 and 333.

5 More than 3 generators

Using obvious definitions, we can extend the concept of daisy chains with three generators to that of daisy chains with n generators where n is an arbitrary positive integer. Computer search has shown that such daisy chains with four generators are not rare. They provide a story for another day.

Acknowledgments

The author is very grateful to E. R. Vaughan (Queen Mary, University of London) for writing the computer program that produced complete listings of 3-generator daisy chains, and to the referee who improved two of the theorems and made many helpful comments.

TABLE 3

Parameters for daisy chains with 3 generators
n composite ($n < 140$)
† marks a composite n that has 3 distinct prime factors
* marks a value that generates $-1 \pmod n$

n	$\xi(n)$	N_n	ψ	ω	π	Notes	Theorem	u	v	w
45	2	4	4	3	2	a, j	3.2, 3.5	28	31	-1
						c	–	28	16	-1
			3	4	2	a, j	3.5	16	37	-1
						b, m	–	31	37	-1
55	2	4	5	4	2	a, j	3.5	31	12	-1
			4	5	2	a, j	3.5	23	16	-1
63	6	16	6	3	2	a, j	3.2, 3.5	19	22	-1
						c	–	19	43	-1
						t	3.3	-2	22	-1
						–	Note 4.1(a)	10	25	-1
			3	6	2	a, j	3.5	43	10	-1
						b, m	–	22	10	-1
						r	–	22	-2	-1
						–	Note 4.1(a)	43	19	-1
			3	2	6	j, s	Note 1.1	46	55	32
65	4	2	4	3	4	n	–	31	16	47*
						j, r	–	31	16	8*
75	2	5	5	4	2	b, j	3.5	31	7	-1
						a	–	61	7	-1
			4	5	2	c, j	3.5	43	46	-1

continued...

Notes (all the congruences being interpreted modulo n):

[a] $u + 2v \equiv 0$
[b] $u^2 \equiv 2vw$
[c] $u + 2v^2 \equiv 0$
[d] $v \equiv u + 1$
[j] $(u + 1)vw \equiv 1$
[k] $u(v + 1)w \equiv 1$
[m] $(u^2 + 1)vw \equiv 1$
[n] $uv(w - 1) \equiv 1$
[o] $u \equiv 2v$
[p] $uw \equiv 2v$
[q] $vw \equiv 2u$
[r] $v \equiv 2w$
[s] $2w \equiv 1$
[t] $u \equiv -2$

TABLE 3 (page 2)

n	$\xi(n)$	N_n	ψ	ω	π	Notes	Theorem	u	v	w
77	2	4	6	5	2	a, j	3.5	12	71	-1
			5	6	2	a, j	3.5	64	45	-1
87	2	3	7	4	2	b, j	3.5	16	46	-1
			4	7	2	c, j	3.5	70	49	-1
91	6	27	12	3	2	$-$	3.1	19	16	-1
			12	2	3	j	$-$	60	27	81
						$-$	$-$	19	-1	16
			6	4	3	n, r	$-$	40	57	74
			4	6	3	n	$-$	57	40	74
			4	3	6	n	$-$	57	79	61
			3	4	6	n	$-$	79	57	61
			3	2	12	j, s	Note 1.1	53	27	46
93	2	5	10	3	2	t	3.1	-2	25	-1
			6	5	2	j	3.5	88	70	-1
			5	6	2	j	3.5	4	37	-1
95	2	4	9	4	2	a, j	3.5	36	77	-1
			4	9	2	a, j	3.5	58	66	-1
99	2	8	10	3	2	b	3.2	19	67	-1
			$\dot{3}$	10	2	c	$-$	34	73	-1
105†	4	4	6	4	2	a, j	3.5	61	22	-1
			4	6	2	a, j	3.5	43	31	-1
115	2	8	11	4	2	o	$-$	71	93	-1
			4	11	2	o	$-$	47	81	-1

continued...

TABLE 3 (page 3)

n	$\xi(n)$	N_n	ψ	ω	π	Notes	Theorem	u	v	w
117	6	46	12	3	2	a, j	3.2, 3.5	37	40	-1
						c	–	37	79	-1
						t	3.3	-2	40	-1
						–	Note 4.1(b)	46	61	-1
			4	3	6	n	–	109	79	113
						j	–	73	79	29
			3	12	2	a, j	3.5	79	19	-1
						b, m	–	40	19	-1
						r	–	40	-2	-1
						–	Note 4.1(a)	79	37	-1
			3	4	6	n, r	–	79	109	113
						k	–	79	73	29
123	2	3	8	5	2	j	3.5	85	10	-1
						b	–	85	16	-1
			5	8	2	j	3.5	37	55	-1
129	2	4	14	3	2	–	3.1	94	79	-1
			7	6	2	j	3.5	121	37	-1
			6	7	2	j	3.5	7	16	-1
133	6	33	18	3	2	–	–	5	30	-1
			18	2	3	–	–	109	-1	102
			9	6	2	a, j	3.5	36	115	-1
						–	Note 4.1(b)	43	68	-1
			9	2	6	j	–	25	-1	46
						–	Note 1.1	36	113	31^*
						–	Note 1.1	99	113	45
			6	9	2	a, j	3.5	96	85	-1
						–	Note 4.1(a)	115	74	-1
			3	2	18	j, s	Note 1.1	39	20	67
135	2	12	9	4	2	a, j	3.5	106	82	-1
						b, m	–	76	82	-1
			4	9	2	a, j	3.5	28	121	-1
						c	–	28	16	-1

References

[1] P. J. Cameron and D. A. Preece, *Notes on Primitive λ-roots*, http://www.maths.qmul.ac.uk/~pjc/csgnotes/lambda.pdf .

[2] R. D. Carmichael, Note on a new number theory function, *Bull. Amer. Math. Soc.* **16** (1909–10), 232–237.

[3] R. D. Carmichael, Generalizations of Euler's ϕ-function, with applications to Abelian groups, *Quart. J. Math.* **44** (1913), 94–104.

[4] G. A. Jones and J. M. Jones, *Elementary Number Theory*. Springer, London, 1998.

[5] D. A. Preece, Daisy chains—a fruitful combinatorial concept, *Australas. J. Combin.* **41** (2008), 297–316.

[6] D. A. Preece, Supplementary Tables for *Daisy Chains with Three Generators*, http://ajc.maths.uq.edu.au/appendices/AJCvol45pp157-174Appendix.pdf .

(Received 27 Aug 2008; revised 26 Jan 2009)