AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **49** (2011), Pages 77–93

Daisy chains with four generators

D. A. Preece* E. R. Vaughan

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

Abstract

For many positive odd integers n, whether prime or not, the set $\mathbb{U}_n$ of units of $\mathbb{Z}_n$ contains members t, u, v and w, say with respective orders τ, ψ, ω and π, such that we can write $\mathbb{U}_n$ as the direct product $\mathbb{U}_n = \langle t\rangle \times \langle u\rangle \times \langle v\rangle \times \langle w\rangle$. Each element of $\mathbb{U}_n$ can then be written in the form $t^h u^i v^j w^k$ where $0 \le h < \tau$, $0 \le i < \psi$, $0 \le j < \omega$ and $0 \le k < \pi$. We can then often use the structure of $\langle t\rangle \times \langle u\rangle \times \langle v\rangle \times \langle w\rangle$ to arrange the $\tau\psi\omega\pi$ elements of $\mathbb{U}_n$ in a *daisy chain*, *i.e.* in a circular arrangement such that, as we proceed once 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 daisy chains based on such 4-factor decompositions as *daisy chains with four generators*. We study the existence of such arrangements, and we note their relationships with the previously studied *daisy chains with three generators*. The smallest prime values n for which daisy chains with four generators exist are 571 and 1051.

1 Introduction

What is the matter with Mary Jane?
I've promised her dolls and a daisy-chain,
And a book about animals — all in vain —
What *is* the matter with Mary Jane?

A. A. Milne [3]

We need the same preliminaries as in our previous study [7] of daisy chains with three generators.

* Also at School of Mathematics, Statistics and Actuarial Science, Cornwallis Building, University of Kent, Canterbury, Kent CT2 7NF, U.K. D.A.Preece@qmul.ac.uk

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 co-prime with n. The number of units in $\mathbb{Z}_n$ is given by *Euler's totient function*

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

(*e.g.* [2, p. 87]). For n odd, a *daisy chain* [6] for the units of $\mathbb{Z}_n$ (in short, a $\mathbb{Z}_n$ daisy chain, or daisy chain for n) 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 [6, 7] and elsewhere, we use square brackets to indicate a cycle. However, also as in [6, 7], 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 $a_{i+1} - a_i$.

For n prime, the cycle $[b_1, b_2, \ldots, b_{n-1}]$ of differences for a $\mathbb{Z}_n$ daisy chain $[a_1, a_2, \ldots, a_{n-1}]$ is an R-*sequencing of* $\mathbb{Z}_n$ [4, §2]. Thus the present paper leads to new structures for R-sequencings. Paige [5] showed that an R-sequencing for a group of order n is sufficient for the construction of a pair of mutually orthogonal $n \times n$ Latin squares. Further details of R-sequencings are in [1, Chapters 2 and 3].

Various systematic methods of construction of $\mathbb{Z}_n$ daisy chains were given in [6]. These included constructions of what, in the terminology of the present paper, could be called *daisy chains with two generators*, each made up of successive *segments*. Then *daisy chains with three generators* were studied in [7], each such daisy chain comprising successive *super-segments* each made up of successive segments. We now make the natural extension to four generators.

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 t, u, v and w, say with respective orders τ, ψ, ω and π, such that we can write $\mathbb{U}_n = \langle t \rangle \times \langle u \rangle \times \langle v \rangle \times \langle w \rangle$. (Here, as subsequently in this paper, the symbol $\times$, when taken in conjunction with angle brackets, indicates a direct product.) All, some or none of the orders τ, ψ, ω and π may be prime. Each element of $\mathbb{U}_n$ can then be written in the form $t^h u^i v^j w^k$ where $0 \leq h \leq \tau - 1$, $0 \leq i \leq \psi - 1$, $0 \leq j \leq \omega - 1$ and $0 \leq k \leq \pi - 1$. We can then often use the structure of $\langle t \rangle \times \langle u \rangle \times \langle v \rangle \times \langle w \rangle$ to arrange the $\tau\psi\omega\pi$ elements of $\mathbb{U}_n$ in a $\mathbb{Z}_n$ daisy chain. We describe daisy chains formed in this way as *daisy chains with four generators* or as *four-generator daisy chains*, the generators being t, u, v and w. Each such daisy chain consists of a succession of *hyper-segments* of length $\psi\omega\pi$, each made up of *super-segments* of length $\omega\pi$, each of which is 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; within each hyper-segment, each successive super-segment is obtained by multiplication by u; each successive hyper-segment is obtained from the preceding one by multiplication by t. When displaying

one of these daisy chains, we use a *single fence* | to denote a boundary between two segments within a supersegment, a *double fence* || to denote a boundary between supersegments, and a *triple fence* ||| to denote a boundary between hypersegments. An example for $n = 91$ is

$$
\begin{array}{rl}
 & \begin{array}{ccc} w & v & u \\ \downarrow & \downarrow & \downarrow \end{array} \\
\hookrightarrow & 1\ 16\ 74 \mid 27\ 68\ 87 \parallel 79\ 81\ 22 \mid 40\ \ 3\ 48 \parallel 53\ 29\ \ 9 \mid 66\ 55\ 61 \vert\vert\vert \\
t\to & 8\ 37\ 46 \mid 34\ 89\ 59 \parallel 86\ 11\ 85 \mid 47\ 24\ 20 \parallel 60\ 50\ 72 \mid 73\ 76\ 33 \vert\vert\vert \\
 & 64\ 23\ \ 4 \mid 90\ 75\ 17 \parallel 51\ 88\ 43 \mid 12\ 10\ 69 \parallel 25\ 36\ 30 \mid 38\ 62\ 82 \vert\vert\vert \\
 & 57\ \ 2\ 32 \mid 83\ 54\ 45 \parallel 44\ 67\ 71 \mid\ \ 5\ 80\ \ 6 \parallel 18\ 15\ 58 \mid 31\ 41\ 19 \vert\vert\vert \hookleftarrow
\end{array}
$$

This has $(\tau, \psi, \omega, \pi) = (4, 3, 2, 3)$ and $(t, u, v, w) = (8, 79, 27, 16)$.

In general, if the first segment of a four-generator daisy chain is

$$\mathcal{S}_w \ = \ w^0 \ \ w^1 \ \ \ldots \ \ w^{\pi-1} \ ,$$

then the first super-segment is

$$\mathcal{S}_{v,w} \ = \ v^0\mathcal{S}_w \mid v^1\mathcal{S}_w \mid \ \cdots \ \mid v^{\omega-1}\mathcal{S}_w \mid \ ;$$

the first hyper-segment is

$$\mathcal{S}_{u,v,w} \ = \ u^0\mathcal{S}_{v,w} \parallel u^1\mathcal{S}_{v,w} \parallel \ \cdots \ \parallel u^{\omega-1}\mathcal{S}_{v,w} \parallel \ ,$$

and the four-generator daisy chain is

$$\hookrightarrow t^0\mathcal{S}_{u,v,w} \ \vert\vert\vert \ t^1\mathcal{S}_{u,v,w} \ \vert\vert\vert \ \ \cdots \ \ \vert\vert\vert \ t^{\omega-1}\mathcal{S}_{u,v,w} \ \vert\vert\vert \ \hookleftarrow \ .$$

Whenever we specify the generators of such a daisy chain, their ordering will always be as above; thus the first segment of the daisy chain will always contain the successive powers of the last generator, and so on.

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

Once hand-working had established that daisy chains with four generators do indeed exist and seem worthy of study, a computer program was written in the programming language C to output, within any chosen range of odd values of n, the sets of parameters $(\tau, \psi, \omega, \pi)$ and (t, u, v, w) for all daisy chains with four generators.

2 Odd prime values of n

Clearly, for an odd prime value of n, the existence of a daisy chain with four generators requires that $n - 1$ can be expressed as the product of four mutually prime

factors. This is not, however, a sufficient requirement; for example, none of the following prime values of n has a daisy chain with four generators: 211, 311, 421, 547, 631, 661, 691, 859, 911, 967, 991, ... The mutually prime factors are not necessarily individually prime or prime power, as can be seen from Table 1, which gives parameter sets for all four-generator daisy chains for prime n in the range $n < 4000$.

For odd prime values of n, many daisy chains with two generators can be constructed where the difference at the end of the first segment is -1 (see [6]). Likewise, for the primes $n = 229, 241, 331, 337, 373, 409, 421, 443, 461, \ldots$, daisy chains with three generators can be constructed in which the difference at the end of the first *super*-segment is -1 (see [7, 8]). We now find that this pattern extends. For odd primes (and commonly, as we see below, for odd composites) there exist daisy chains with four generators such that the difference at the end of the first *hyper*-segment is -1. We then have $t - (uvw)^{-1} \equiv -1 \pmod{n}$, whence $(t+1)uvw \equiv 1 \pmod{n}$. The smallest primes for which this property holds are $n = 1321$, 3499 and 3931 (see Table 1). No pattern for the occurrence of this property is apparent.

If n is an odd prime for which there exists a four-generator daisy chain with $\omega = 3$ and $\pi = 2$, then $v^2 + v + 1 \equiv 0$ and $w \equiv -1 \pmod{n}$. Thus $v^2 - vw \equiv v^2 + v \equiv -1 \pmod{n}$, whence -1 is the difference at the end of the second segment. Many occurrences of this can be found in Table 1, but again no general result covering these occurrences is detectable.

3 Odd composite values of n

For odd composite values n, the existence of a daisy chain with four generators requires that the prime-power decomposition of n contains no more than four distinct primes. In fact, daisy chains with four generators exist in abundance for some odd composite values n for which the prime-power decomposition contains just two or three distinct primes. The abundance tends to be greater when at least one of the primes in the prime-power decomposition is raised to a power greater than 1.

As mentioned above, many four-generator daisy chains for composite n have -1 as the difference at the end of the first hyper-segment, so that $(t+1)uvw \equiv 1 \pmod{n}$. This property may even be satisfied by different daisy chains with the same parameter-set $(n, \tau, \psi, \omega, \pi)$, *e.g.* for $(n, \tau, \psi, \omega, \pi) = (275, 5, 5, 4, 2)$, for which the possibilities with this property include $(t, u, v, w) = (56, 126, 232, -1)$ and $(141, 221, 232, -1)$. If a four-generator daisy chain has this property and the values of the three parameters ψ, ω and π are co-prime, then there is a two-generator daisy chain $\hookrightarrow \langle t \rangle_\tau \times \langle uvw \rangle_{\psi\omega\pi} \hookleftarrow$ corresponding to the decomposition $\langle t \rangle \times \langle t+1 \rangle = \langle t \rangle \times \langle u^{-1}v^{-1}w^{-1} \rangle$ of $\mathbb{U}_n$.

Example 3.1: The daisy chain $\hookrightarrow \langle 118 \rangle_4 \times \langle 46 \rangle_5 \times \langle 76 \rangle_3 \times \langle -1 \rangle_2 \hookleftarrow$ for $n = 225$ (see Table 2) has $(t+1)uvw \equiv 1 \pmod{n}$ and corresponds to the daisy chain $\hookrightarrow \langle 118 \rangle_4 \times \langle 104 \rangle_{30} \hookleftarrow$. ◇

Table 1: Parameters for daisy chains with four generators, n prime, $n < 4000$
(Within each pair of sets of values (t, u, v, w), the values t, u, v, w in the second set are the inverses of those in the first.)

n	N_n	τ	ψ	ω	π	t	u	v	w	
571	2	19	5	3	2	64	167	461	-1	
						116	106	109	-1	
		19	3	5	2	64	461	167	-1	
						116	109	106	-1	
1051	1	25	7	3	2	405	801	180	-1	
						737	845	870	-1	
1303	1	31	7	2	3	419	52	-1	1207	
						1048	426	-1	95	
1321	1	11	5	3	8	884	516	297	235	$(t{+}1)uvw \equiv 1 (\mathrm{mod}\ n)$
						925	1257	1023	950	
1723	3	41	7	3	2	262^i	1261	41	-1	$i = 1,\ 18$
						1335^i	317	1681	-1	
		41	2	3	7	351	-1	41	317	
						54	-1	1681	1261	
1831	5	61	2	5	3	515^i	-1	123	672	$i = 1,\ 15,\ 22,\ 42,\ 58$
						32^i	-1	655	1158	
1861	1	31	4	5	3	452	61	739	454	
						1264	1800	768	1406	
2131	6	71	5	3	2	207^i	2046	1662	-1	$i = 1,\ 2,\ 58$
						978^i	1780	468	-1	
		71	5	2	3	207^i	2046	-1	1662	$i = 1,\ 2,\ 58$
						978^i	1780	-1	468	
2311	3	77	3	5	2	1514	1428	585	-1	
						1531	882	1833	-1	
		77	2	5	3	298^i	-1	585	882	$i = 1,\ 29$
						380^i	-1	1833	1428	

continued...

Table 1 (page 2)

n	N_n	τ	ψ	ω	π	t	u	v	w	
2347	3	23	17	3	2	19^i	784^j	1062	-1	$(i,j) = (1,1),\ (7,6),$
						2100^i	470^j	1284	-1	$(15,10)$
2371	1	79	5	3	2	1089	971	1906	-1	
						2199	1238	464	-1	
2591	1	37	5	2	7	762	657	-1	891	
						2574	2311	-1	474	
2707	1	41	11	3	2	1288	235	1327	-1	
						2583	599	1379	-1	
2731	3	65	7	3	2	549^i	2668	2284	-1	$i = 1,\ 27,\ 33$
						1756^i	1864	446	-1	
2851	4	19	25	3	2	729^i	789^j	1836	-1	$(i,j) = (1,1),\ (3,8)$
						2237^i	430^j	1014	-1	
		19	25	2	3	729^i	789^j	-1	1836	$(i,j) = (1,1),\ (3,8)$
						2237^i	430^j	-1	1014	
3011	1	43	5	7	2	828	1248	1577	-1	
						2971	2058	2253	-1	
3319	5	79	3	7	2	296^i	1791	2623	-1	$i = 1,\ 40,\ 53,\ 77$
						2792^i	1527	1979	-1	
		7	79	2	3	441	520	-1	1791	
						1731	517	-1	1527	
3361	2	32	5	7	3	1031	200	2898	892	
						2295	2672	3165	2468	
		32	5	3	7	1031	200	892	2898	
						2295	2672	2468	3165	

continued...

Table 1 (page 3)

n	N_n	τ	ψ	ω	π	t	u	v	w	
3499	8	53	11	3	2	847^i	223^j	3342	-1	$(i,j)=(1,1),\ (11,1),$
						1450^i	2840^j	156	-1	$(4,-1)$
		53	11	2	3	847^i	223^j	-1	3342	$(i,j)=(1,1),\ (11,1),$
						1450^i	2840^j	-1	156	$(4,-1)$
		53	3	11	2	3127	3342	2528	-1	$(t{+}1)uvw\equiv 1 \pmod n$
						2549	156	1236	-1	
		53	3	2	11	3127	3342	-1	2528	$(t{+}1)uvw\equiv 1 \pmod n$
						2549	156	-1	1236	
3571	2	85	7	3	2	720^i	654	103	-1	$i=1,\ 14$
						739^i	1305	3467	-1	
3613	2	43	7	3	4	201^i	3177	1937	85	$i=1,\ 6$
						2894^i	2428	1675	3528	
3631	11	121	5	2	3	19^i	847	-1	3295	$i=1,\ 13,\ 56,\ 69,$
						1720^i	3108	-1	335	$85,\ 91,\ 102$
		121	2	3	5	19^i	-1	3295	1204	$i=24,\ 82,\ 90,$
						1720^i	-1	335	2102	104
3697	1	16	11	7	3	2621	1192	582	519	
						3563	1436	2128	3177	
3907	2	31	7	9	2	531^i	1883	1562	-1	$i=1,\ 13$
						3105^i	3048	2929	-1	
3931	13	131	3	5	2	374^i	617	3834	-1	$i=1,\ 69,\ 71,\ 77,\ 124$
						3437^i	3313	3161	-1	
		131	3	2	5	374^i	617	-1	3834	$i=1,\ 69,\ 71,\ 77,\ 124$
						3437^i	3313	-1	3161	
		131	2	5	3	374^i	-1	1547	617	$i=1,\ 56,\ 94$
						3437^i	-1	3250	3313^*	

* with $i=94$, *i.e.* with $3437^i=733$, this daisy chain has $(t{+}1)uvw\equiv 1 \pmod n$

We may also have -1 as the difference at the end of the first *super*-segment, so that $(u+1)vw \equiv 1 \pmod{n}$. This too occurs in several daisy chains with $(n, \tau, \psi, \omega, \pi) = (275, 5, 5, 4, 2)$, for which the possibilities include $(t, u, v, w) = (16, 31, 232, -1)$ and $(56, 31, 232, -1)$. Likewise -1 can be the difference at the end of the first segment, so that $(v+1)w \equiv 1 \pmod{n}$. This occurs, for example, with $(n, \tau, \psi, \omega, \pi) = (91, 3, 2, 4, 3)$ and $(259, 3, 2, 4, 9)$, for which we can have $(t, u, v, w) = (53, 27, 8, 81)$ and $(186, 223, 43, 53)$ respectively.

Another possibility that occurs sufficiently frequently to merit comment is $(tu+1)vw \equiv 1 \pmod{n}$. This relationship often holds in conjunction with $(t-1)(u-1) \equiv 0 \pmod{n}$, and we then also have $(t+u)vw \equiv 1 \pmod{n}$. Then $t^{-1}u - t^{-1}v^{-1}w^{-1} \equiv -1$, so that -1 is the difference at the end of the *first* super-segment of the *last* hyper-segment.

Other relationships that occur frequently for four-generator daisy chains for composite n include $t(u+1)vw \equiv 1$ and $tu(v+1)w \equiv 1 \pmod{n}$.

For odd composite integers n in the range $n < 350$, there are so many four-generator daisy chains that we cannot give full details. Indeed, throughout Table 2 we mostly give only one set of parameters (t, u, v, w) for each parameter-set $(n, \tau, \psi, \omega, \pi)$ for which a four-generator daisy chain exists. Exceptions are made in order to include occurrences of $(tu+1)vw \equiv 1 \pmod{n}$. Table 2 is annotated to draw attention to frequently occurring types of relationship between parameters (t, u, v, w), but once again no general results are revealed.

4 Refinements

We now examine how a four-generator daisy chain may be related to one or more three-generator daisy chains with which it has two generators in common. To do this we need further notation and definitions. We write

$$\hookrightarrow \ \langle t \rangle \times \langle u \rangle \times \langle v \rangle \times \langle w \rangle \ \hookleftarrow \tag{1}$$

for a four-generator daisy chain where the ordering of the generators t, u, v and w is as above. Similarly we write

$$\hookrightarrow \ \langle a \rangle \times \langle b \rangle \times \langle c \rangle \ \hookleftarrow$$

for a three-generator daisy chain where the generators a, b and c are similarly ordered (so that the elements c^0, c^1, c^2, ... come first in the daisy chain, in that order). If, for some value of n, there exist the four-generator daisy chain (1) and any one or more of the three-generator daisy chains

$$\hookrightarrow \ \langle tu \rangle \times \langle v \rangle \times \langle w \rangle \ \hookleftarrow , \tag{2}$$

$$\hookrightarrow \ \langle t \rangle \times \langle uv \rangle \times \langle w \rangle \ \hookleftarrow \tag{3}$$

Table 2: Specimen sets of parameters for daisy chains with four generators, n odd and neither prime nor a prime power, $n < 350$

n	N_n	τ	ψ	ω	π	t	u	v	w	Note
$91 = 7 \times 13$	6	4	3	2	3	8	53	27	81	h, i
		3	4	2	3	53	8	27	81	h, i
		3	2	4	3	53	27	8	81	g
$171 = 3^2 \times 19$	6	9	2	3	2	82	37	49	-1	j
$195 = 3 \times 5 \times 13$	2	4	3	4	2	31	16	187	-1	j
$217 = 7 \times 31$	2	10	3	2	3	15	191	-1	149	$*$
$225 = 3^2 \times 5^2$	30	5	4	3	2	136	118	76	-1	h
						181	82	76	-1	j
		5	3	4	2	181	151	82	-1	h, i
						181	76	82	-1	j
		4	5	3	2	118	46	76	-1	j
		4	3	5	2	118	151	46	-1	h, i
						118	76	46	-1	j
		3	5	4	2	151	181	82	-1	h, i
						151	91	82	-1	j
		3	4	5	2	151	118	46	-1	h, i
						76	118	46	-1	k
$247 = 13 \times 19$	21	9	4	2	3	196	229	170	68	k
		9	2	4	3	196	170	229	68	ℓ
		4	9	2	3	229	196	170	68	j
$259 = 7 \times 37$	7	9	2	4	3	44	-1	43	121	j
		4	3	2	9	43	186	223	53	h, i
		3	4	2	9	186	43	223	53	h, i
		3	2	4	9	186	223	43	53	g

continued...

Notes (all congruences being modulo n):

* the difference -1 lies within a segment

^{g} $(v+1)w \equiv 1$ ^{h} $(tu+1)vw \equiv 1$ ^{i} $(t+u)vw \equiv 1$

^{j} $(t+1)uvw \equiv 1$ ^{k} $t(u+1)vw \equiv 1$ $^\ell$ $tu(v+1)w \equiv 1$ ^{m} $(t+1)vw \equiv u$

Table 2 (page 2)

n	N_n	τ	ψ	ω	π	t	u	v	w	Note
$261 = 3^2 \times 29$	18	7	4	3	2	82	244	175	-1	h
						136	244	175	-1	k
		7	3	4	2	190	88	46	-1	h, i
						226	88	46	-1	k
		4	7	3	2	244	136	175	-1	j
		4	3	7	2	244	88	136	-1	h, i
						244	175	136	-1	j
		3	7	4	2	88	190	46	-1	h, i
						88	226	46	-1	j
		3	4	7	2	88	244	136	-1	h, i
						175	244	136	-1	k
$273 = 3 \times 7 \times 13$	18	6	4	3	2	199	265	79	-1	j
		4	6	3	2	190	166	79	-1	j
		4	3	6	2	190	22	199	-1	j
		4	3	2	6	190	235	118	263	h, i
		3	4	6	2	79	265	82	-1	m
		3	4	2	6	235	190	118	263	h, i
		3	2	12	2	235	118	136	-1	j
		3	2	4	6	235	118	190	263	g
$275 = 5^2 \times 11$	186	5	5	4	2	56	126	232	-1	j
		5	4	5	2	126	243	196	-1	h, i
						56	232	126	-1	j
		5	2	5	4	201	76	91	43	j
		4	5	5	2	243	126	196	-1	h, i
						232	56	126	-1	k

continued...

Table 2 (page 3)

n	N_n	τ	ψ	ω	π	t	u	v	w	Note
$279 = 3^2 \times 31$	106	15	2	3	2	262	154	67	-1	$-$
		10	3	3	2	91	67	118	-1	j
		6	5	3	2	37	190	94	-1	k
		6	3	5	2	274	187	163	-1	j
		5	6	3	2	190	37	94	-1	j
		5	3	6	2	190	94	223	-1	h, i
						190	94	37	-1	j
		3	10	3	2	94	91	118	-1	$-$
		3	6	5	2	94	37	190	-1	ℓ
		3	5	6	2	94	190	223	-1	h, i
						94	190	37	-1	k
$301 = 7 \times 43$	18	14	3	2	3	204	44	216	135	$-$
		7	6	3	2	127	178	36	-1	j
		7	3	6	2	127	36	178	-1	j
		7	3	2	6	127	92	85	208	$*$
		3	14	2	3	44	204	216	135	$-$
		3	2	14	3	44	216	204	135	$-$
$309 = 3 \times 103$	3	17	2	3	2	79	205	262	-1	$-$
$315 = 3^2 \times 5 \times 7$	120	12	2	3	2	73	181	121	-1	j
		6	4	3	2	271	127	211	-1	j
		6	3	4	2	271	211	127	-1	j
		4	6	3	2	253	136	211	-1	j
		4	3	6	2	253	211	136	-1	j
		4	3	2	6	127	226	181	149	k
		3	6	4	2	211	241	127	-1	j
		3	4	6	2	211	127	241	-1	j
		3	4	2	6	226	127	181	149	j
		3	2	12	2	46	181	157	-1	j
		3	2	4	6	226	181	127	149	j

continued...

Table 2 (page 4)

n	N_n	τ	ψ	ω	π	t	u	v	w	Note
$319 = 11 \times 29$	18	7	5	4	2	23	262	133	-1	k
		7	4	5	2	111	12	291	-1	h
						45	133	291	-1	j
		5	7	4	2	262	23	133	-1	j
		5	4	7	2	291	12	78	-1	k
		4	7	5	2	12	78	291	-1	j
		4	5	7	2	12	291	78	-1	j
$325 = 5^2 \times 13$	24	5	4	3	4	131	226	276	268	h, i
						66	226	276	268	k
		4	5	3	4	226	131	276	268	h, i
						226	66	276	268	j
		4	3	5	4	226	276	66	268	j
$333 = 3^2 \times 37$	6	9	4	3	2	118	154	121	-1	j
$335 = 5 \times 67$	18	11	4	3	2	76	68	96	-1	–
		11	3	4	2	76	96	68	-1	–
		4	11	3	2	68	76	96	-1	m
$341 = 11 \times 31$	133	15	2	5	2	100	309	159	-1	j
		10	5	3	2	23	16	67	-1	–
		10	3	5	2	23	67	225	-1	j
		6	5	5	2	243	218	287	-1	h, i
						243	78	16	-1	j
		6	5	2	5	254	163	-1	225	–
		5	10	3	2	218	23	56	-1	–
		5	6	5	2	218	243	287	-1	h, i
						163	254	221	-1	j
		5	5	6	2	163	221	254	-1	j
		5	3	10	2	287	56	27	-1	j
		5	3	2	10	78	56	309	171	h
						188	67	309	281	j
		5	2	15	2	125	32	9	-1	–
		5	2	3	10	188	309	67	281	j

and

$$\hookrightarrow\ \langle t\rangle \times \langle u\rangle \times \langle vw\rangle\ \hookleftarrow\ , \tag{4}$$

then we say that the daisy chain (1) is a *refinement* of any daisy chain (2), (3) or (4). To specify the orders of generators, modulo n, we use subscripts as in

$$\hookrightarrow\ \langle t\rangle_\tau \times \langle u\rangle_\psi \times \langle v\rangle_\omega \times \langle w\rangle_\pi\ \hookleftarrow\ .$$

Clearly, if this last four-generator daisy chain exists, it can be a refinement of a daisy chain (2) only if τ and ψ are co-prime. Likewise the existence of (3) requires ψ and and ω to be co-prime, and that of (4) requires ω and π to be co-prime.

Example 4.1 For $n = 315 = 3^2 \times 5 \times 7$ there exists (see Table 2) the daisy chain

$$\hookrightarrow\ \langle 211\rangle_3 \times \langle 241\rangle_6 \times \langle 127\rangle_4 \times \langle -1\rangle_2\ \hookleftarrow\ .$$

Examination of the orders of the successive generators shows that this four-generator daisy chain is not the refinement of any three-generator daisy chain. ◇

Example 4.2 For $n = 91 = 7 \times 13$ there exists (again see Table 2) the daisy chain

$$\hookrightarrow\ \langle 8\rangle_4 \times \langle 53\rangle_3 \times \langle 27\rangle_2 \times \langle 81\rangle_3\ \hookleftarrow\ ,$$

which is as follows:

$$\begin{array}{lrrrcrrrcrrrcrrrcrrrcrrrl}
\hookrightarrow & 1 & 81 & 9 & | & 27 & 3 & 61 & || & 53 & 16 & 22 & | & 66 & 68 & 48 & || & 79 & 29 & 74 & | & 40 & 55 & 87 & ||| \\
 & 8 & 11 & 72 & | & 34 & 24 & 33 & || & 60 & 37 & 85 & | & 73 & 89 & 20 & || & 86 & 50 & 46 & | & 47 & 76 & 59 & ||| \\
 & 64 & 88 & 30 & | & 90 & 10 & 82 & || & 25 & 23 & 43 & | & 38 & 75 & 69 & || & 51 & 36 & 4 & | & 12 & 62 & 17 & ||| \\
 & 57 & 67 & 58 & | & 83 & 80 & 19 & || & 18 & 2 & 71 & | & 31 & 54 & 6 & || & 44 & 15 & 32 & | & 5 & 41 & 45 & |||\ \hookleftarrow
\end{array}$$

This is a refinement of the following daisy chain $\hookrightarrow \langle 8\rangle_4 \times \langle 53\rangle_3 \times \langle 3\rangle_6 \hookleftarrow$, the last generator of which comes from the equivalence $3 \equiv 27 \times 81 \pmod{91}$:

$$\begin{array}{lrrrrrrcrrrrrrcrrrrrrl}
\hookrightarrow & 1 & 3 & 9 & 27 & 81 & 61 & | & 53 & 68 & 22 & 66 & 16 & 48 & | & 79 & 55 & 74 & 40 & 29 & 87 & || \\
 & 8 & 24 & 72 & 34 & 11 & 33 & | & 60 & 89 & 85 & 73 & 37 & 20 & | & 86 & 76 & 46 & 47 & 50 & 59 & || \\
 & 64 & 10 & 30 & 90 & 88 & 82 & | & 25 & 75 & 43 & 38 & 23 & 69 & | & 51 & 62 & 4 & 12 & 36 & 17 & || \\
 & 57 & 80 & 58 & 83 & 67 & 19 & | & 18 & 54 & 71 & 31 & 2 & 6 & | & 44 & 41 & 32 & 5 & 15 & 45 & ||\ \hookleftarrow
\end{array}$$

This in turn is a refinement of $\hookrightarrow \langle 60\rangle_{12} \times \langle 3\rangle_6 \hookleftarrow$. The four-generator daisy chain is also a refinement of $\hookrightarrow \langle 8\rangle_4 \times \langle 66\rangle_6 \times \langle 81\rangle_3 \hookleftarrow$ and of $\hookrightarrow \langle 60\rangle_{12} \times \langle 27\rangle_2 \times \langle 81\rangle_3 \hookleftarrow$. ◇

Clearly, the definitions of 3- and 4-generator daisy chains can be generalised in the obvious way to define m-generator daisy chains ($m \geq 1$). The definition of a refinement can likewise be generalised to enable us to pass from an m- to an $(m+1)$-generator daisy chain.

In general, checking that a given m-generator daisy chain $\mathcal{D}$ for n has an $(m+1)$-generator refinement is not easy. However, we now give rules for two simple special cases. We use f to denote the first generator of $\mathcal{D}$, and F to denote the product, modulo n, of the other $m-1$ generators.

Rule 1 *Suppose that the order of f, modulo n, is $3k$ $(k > 1)$ where $k \equiv 1 \pmod 3$. Then $\mathcal{D}$ has a refinement $\mathcal{E}$ where the first generator is f^k (with order 3) and the second is f^{2k+1} (with order k) if and only if $(f^k - 1)(f^{2k-1} + F) \equiv 0 \pmod n$.*

Proof The order of f^{2k+1}, modulo n, is k as $2k + 1$ is a multiple of 3.

For $\mathcal{D}$, the differences between the first element of a super-segment and the preceding element are

$$f^i - f^{i-1}F^{-1} \quad (i = 1, 2, \ldots, 3k) \; . \tag{5}$$

For $\mathcal{E}$ the differences between the first element of a hyper-segment and the preceding element are three of the differences (5), namely

$$f^j - f^{j-1}F^{-1} \quad (j = k, 2k, \ldots, 3k) \; .$$

Also in $\mathcal{E}$, the difference between the first element of the second super-segment and the preceding element is $f^{2k+1} - F^{-1}$, which must now be matched with a difference from (5) in such a way that the relevant differences for $\mathcal{D}$ and $\mathcal{E}$ are the same. This can be achieved if and only if

$$f^{2k+1} - F^{-1} \equiv f^{k+1} - f^k F^{-1} \pmod n \; .$$

This congruence can be rearranged as

$$f^{k+1}(f^k - 1) + (f^k - 1)F^{-1} \equiv 0 \; ,$$

i.e.

$$(f^k - 1)(f^{k+1} + F^{-1}) \equiv 0 \; ,$$

i.e.

$$(f^k - 1)(F + f^{2k-1}) \equiv 0 \pmod n \; . \qquad \square$$

Example 4.3 For $n = 91 = 7 \times 13$, the existence of $\hookrightarrow \langle 60 \rangle_{12} \times \langle 27 \rangle_2 \times \langle 81 \rangle_3 \hookleftarrow$ implies the existence of the daisy chain $\hookrightarrow \langle 53 \rangle_3 \times \langle 8 \rangle_4 \times \langle 27 \rangle_2 \times \langle 81 \rangle_3 \hookleftarrow$. Here we take $k = 4$ in Rule 1. We have $f = 60$ and $F = 27 \times 81 \equiv 3 \pmod n$, so that $(f^4 - 1)(f^7 + F) \equiv 52 \times 21 \equiv 0 \pmod n$. $\diamond$

Example 4.4 For $n = 261 = 3^2 \times 29$, as $\hookrightarrow \langle 16 \rangle_{21} \times \langle 46 \rangle_4 \times \langle -1 \rangle_2 \hookleftarrow$ exists, so does $\hookrightarrow \langle 88 \rangle_3 \times \langle 190 \rangle_7 \times \langle 46 \rangle_4 \times \langle -1 \rangle_2 \hookleftarrow$. Here we take $k = 7$ along with $f = 16$ and $F \equiv 215 \pmod n$, so that $(f^7 - 1)(f^{13} + F) = 87 \times (223 + 215) \equiv 87 \times 177 = 3 \times 29 \times 3 \times 59 \equiv 0 \pmod n$. $\diamond$

Example 4.5 For $n = 315 = 3^2 \times 5 \times 7$, the existence of the 4-generator daisy chain

$$\hookrightarrow \langle 73 \rangle_{12} \times \langle 181 \rangle_2 \times \langle 151 \rangle_3 \times \langle (-1) \rangle_2 \hookleftarrow$$

(which is *not* the example in Table 2), implies the existence of the 5-generator daisy chain

$$\hookrightarrow \langle 46 \rangle_3 \times \langle 118 \rangle_4 \times \langle 181 \rangle_2 \times \langle 151 \rangle_3 \times \langle (-1) \rangle_2 \hookleftarrow \; . \qquad \diamond$$

Rule 2 *Suppose that the order of f, modulo n, is $3k$ $(k > 1)$ where $k \equiv 2 \pmod 3$. Then $\mathcal{D}$ has a refinement $\mathcal{E}$ where the first generator is f^{2k} (with order 3) and the second is f^{k+1} (with order k) if and only if $(f^k - 1)(f^{k-1} + F) \equiv 0 \pmod n$.*

Proof This is similar to the proof for Rule 1. □

Example 4.6 For $n = 91 = 7 \times 13$, as $\hookrightarrow \langle 66\rangle_6 \times \langle 8\rangle_4 \times \langle 81\rangle_3 \hookleftarrow$ exists, so does $\hookrightarrow \langle 53\rangle_3 \times \langle 27\rangle_2 \times \langle 8\rangle_4 \times \langle 81\rangle_3 \hookleftarrow$. ◇

Example 4.7 For $n = 273 = 3 \times 7 \times 13$ we have the four-generator daisy chain $\hookrightarrow \langle 199\rangle_6 \times \langle 265\rangle_4 \times \langle 79\rangle_3 \times \langle 272\rangle_2 \hookleftarrow$ (see Table 2). With $k = 2$, $f = 199$ and $F = 86$ we have $(f^k - 1)(f^{k-1} + F) \equiv 180 \pmod{273}$. Thus no refinement exists having a first generator of order 3. ◇

5 Lifts

Let

$$\hookrightarrow \langle t\rangle_\tau \times \langle u\rangle_\psi \times \langle v\rangle_\omega \times \langle w\rangle_\pi \hookleftarrow \tag{6}$$

be a four-generator daisy chain for some value n with $n = ab$, where a and b are positive integers greater than 1 that are not necessarily co-prime. Let t^*, u^*, v^* and w^* be the values of t, u, v and w respectively when reduced modulo b. Suppose that a daisy chain for $n = b$ is provided by

$$\hookrightarrow \langle t^*\rangle \times \langle u^*\rangle \times \langle v^*\rangle \times \langle w^*\rangle \hookleftarrow \tag{7}$$

where at least one generator is congruent to 1 (mod b) and so can be ignored. We then say that daisy chain (6) is a *weak lift* of daisy chain (7). Weak lifts are similarly defined for daisy chains with other numbers of generators.

Amongst daisy chains with four generators, the simplest weak lifts are those for which just one of the values t^*, u^*, v^* and w^* is congruent to 1 (mod b), and each generator not congruent to 1 (mod b) has the same order as the corresponding value t, u, v or w.

Example 5.1 The daisy chain

$$\hookrightarrow \langle 181\rangle_5 \times \langle 82\rangle_4 \times \langle 76\rangle_3 \times \langle -1\rangle_2 \hookleftarrow \qquad (n = 225 = 3^2 \times 5^2)$$

(see Table 2) is a weak lift of the daisy chain

$$\hookrightarrow \langle 31\rangle_5 \times \langle 7\rangle_4 \times \langle 1\rangle_1 \times \langle -1\rangle_2 \hookleftarrow \qquad (n = 75 = 3 \times 5^2)\,,$$

and also of the daisy chain

$$\hookrightarrow \langle 1\rangle_1 \times \langle 37\rangle_4 \times \langle 31\rangle_3 \times \langle -1\rangle_2 \hookleftarrow \qquad (n = 45 = 3^2 \times 5)\,.$$

Each of these last two daisy chains is in turn a weak lift of the daisy chain

$$\hookrightarrow \langle 7\rangle_4 \times \langle -1\rangle_2 \hookleftarrow \qquad (n = 15)\,. \qquad \diamond$$

Example 5.2 The daisy chain

$$\hookrightarrow \langle 8\rangle_4 \times \langle 53\rangle_3 \times \langle 27\rangle_2 \times \langle 81\rangle_3 \hookleftarrow \qquad (n = 91 = 7 \times 13)$$

is a weak lift of the daisy chain

$$\hookrightarrow \langle 8\rangle_4 \times \langle 3\rangle_3 \hookleftarrow \qquad (n = 13)\,,$$

but is not a weak lift of a daisy chain for $n = 7$. $\diamond$

If n is a particular value of the form $n = c^2d$, then some, all or none of the daisy chains for n may be weak lifts of daisy chains for $n = cd$. For example, no four-generator daisy chain for $n = 171 = 3^2 \times 19$ is a weak lift of a daisy chain for $n = 57 = 3\times 19$. Contrariwise, every four-generator daisy chain for $n = 261 = 3^2\times 29$ is a weak lift of a daisy chain for $n = 87 = 3 \times 29$, whereas examination of Table 2 shows that some, but not all, four-generator daisy chains for $n = 279 = 3^2 \times 31$ are weak lifts of daisy chains for $n = 93 = 3 \times 31$.

Now let (6) and (7) be daisy chains as before, except that none of the values t^*, u^*, v^* and w^* is congruent to 1 (mod b), and the order (mod b) of one or more of them is a proper factor of the order (mod ab) of the corresponding value t, u, v or w. We now say that the daisy chain (6) is a *strong lift* of daisy chain (7). As above, strong lifts are similarly defined for daisy chains with other numbers of generators.

Example 5.3 The daisy chain

$$\hookrightarrow \langle 235\rangle_3 \times \langle 118\rangle_2 \times \langle 148\rangle_4 \times \langle 74\rangle_6 \hookleftarrow \qquad (n = 273 = 3 \times 7 \times 13)$$

is a strong lift of the daisy chain

$$\hookrightarrow \langle 53\rangle_3 \times \langle 27\rangle_2 \times \langle 57\rangle_4 \times \langle 74\rangle_3 \hookleftarrow \qquad (n = 91 = 7 \times 13)\,. \qquad \diamond$$

6 Permuting the generators

For some values of n, two or more four-generator daisy chains may have different orderings of the same set of generators. Thus, as we see from the start of Table 1,

$$\hookrightarrow \langle 64\rangle_{19} \times \langle 167\rangle_5 \times \langle 461\rangle_3 \times \langle -1\rangle_2 \hookleftarrow$$

and

$$\hookrightarrow \langle 64\rangle_{19} \times \langle 461\rangle_3 \times \langle 167\rangle_5 \times \langle -1\rangle_2 \hookleftarrow$$

are both daisy chains for $n = 571$. We have no general results to indicate when different orderings are possible. But a striking special result is this: for some composite values of n there are four-generator daisy chains that remain daisy chains under any of the 6 permutations of the first three generators. Examples are as follows:

$$\begin{aligned}
n = 225: &\quad \hookrightarrow \langle 46\rangle_5 \times \langle 118\rangle_4 \times \langle 76\rangle_3 \times \langle -1\rangle_2 \hookleftarrow \\
n = 261: &\quad \hookrightarrow \langle 190\rangle_7 \times \langle 46\rangle_4 \times \langle 88\rangle_3 \times \langle -1\rangle_2 \hookleftarrow \\
n = 275: &\quad \hookrightarrow \langle 126\rangle_5 \times \langle 56\rangle_5 \times \langle 232\rangle_4 \times \langle -1\rangle_2 \hookleftarrow \\
n = 279: &\quad \hookrightarrow \langle 37\rangle_6 \times \langle 190\rangle_5 \times \langle 94\rangle_3 \times \langle -1\rangle_2 \hookleftarrow \\
n = 315: &\quad \hookrightarrow \langle 31\rangle_6 \times \langle 127\rangle_4 \times \langle 211\rangle_3 \times \langle -1\rangle_2 \hookleftarrow \\
n = 319: &\quad \hookrightarrow \langle 78\rangle_7 \times \langle 262\rangle_5 \times \langle 12\rangle_4 \times \langle -1\rangle_2 \hookleftarrow \\
n = 341: &\quad \hookrightarrow \langle 243\rangle_6 \times \langle 287\rangle_5 \times \langle 218\rangle_5 \times \langle -1\rangle_2 \hookleftarrow
\end{aligned}$$

7 Daisy chains with more generators

Example 4.5 indicates that n need not be vast for a daisy chain with 5 generators. Further study of m-generator daisy chains, $m \geq 5$, is however beyond the scope of this paper.

References

[1] J. Dénes and A. D. Keedwell, *Latin squares: New Developments in the Theory and Applications*. North-Holland, Amsterdam, 1991.

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

[3] A. A. Milne, Rice Pudding, in: *When We Were Very Young*. Methuen, London, 1924.

[4] M. A. Ollis, On terraces for abelian groups, *Discrete Math.* **305** (2005), 250–263.

[5] L. J. Paige, Complete mappings of finite groups, *Pacific J. Math.* **1** (1951), 111–116.

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

[7] D. A. Preece, Daisy chains with three generators, *Australas. J. Combin.* **45** (2009), 157–174.

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

(Received 27 Oct 2009; revised 4 Nov 2010)