View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Discrete Mathematics 293 (2005) 29–59

ELSEVIER

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Some power-sequence terraces for $\mathbb{Z}_{pq}$ with as few segments as possible

Ian Anderson[a], D.A. Preece[b, c]

[a] *Department of Mathematics, University of Glasgow, University Gardens, Glasgow G12 8QW, UK*
[b] *School of Mathematical Sciences, Queen Mary, University of London, Mile End Road, London E1 4NS, UK*
[c] *Institute of Mathematics, Statistics and Actuarial Science, Cornwallis Building, University of Kent, Canterbury, Kent CT2 7NF, UK*

Received 2 July 2003; received in revised form 31 May 2004; accepted 18 August 2004
Available online 19 March 2005

Abstract

A power-sequence terrace for $\mathbb{Z}_n$ is a $\mathbb{Z}_n$ terrace that can be partitioned into segments one of which contains merely the zero element of $\mathbb{Z}_n$ whilst each other segment is either (a) a sequence of successive powers of an element of $\mathbb{Z}_n$, or (b) such a sequence multiplied throughout by a constant. If $n = pq$, where p and q are distinct odd primes, the minimum number of segments for such a terrace is $3+\xi(n)$, where $\xi(n)$ is the ratio $\phi(n)/\lambda(n)$ of the number of units in $\mathbb{Z}_n$ to the maximum order of a unit from $\mathbb{Z}_n$. For $n = pq$, general constructions are provided for power-sequence $\mathbb{Z}_n$ terraces with $3 + \xi(n)$ segments. These constructions are for $\xi(n) = 2$, 4 and 6, and they produce terraces throughout the range $n < 200$ except for $n = 119, 161$.
© 2005 Elsevier B.V. All rights reserved.

MSC: 10A07 (05B30)

Keywords: Carmichael's λ-function; Euler's function; Power-sequence terraces; Primitive roots; Primitive λ-roots; Units of $\mathbb{Z}_n$

1. Introduction

Let G be a finite group of order n with identity element e, let the group operation be multiplication, let $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ be an arrangement of the elements of G, and let

E-mail address: ia@maths.gla.ac.uk (I. Anderson).

0012-365X/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2004.08.020

$\mathbf{b}=(b_1, b_2, \ldots, b_n)$ be the ordered sequence where $b_1=e$ and $b_i=a_{i-1}^{-1}a_i$ for $i=2, 3, \ldots, n$. Bailey [5] defined the arrangement **a** to be a *terrace* for G, with **b** as the corresponding 2-*sequencing* or *quasi-sequencing* for G, if **b** contains exactly one occurrence of each element $x \in G$ that satisfies $x = x^{-1}$, and if, for each $x \in G$ that satisfies $x \neq x^{-1}$, the sequence **b** contains exactly two occurrences of x but none of x^{-1}, or exactly two occurrences of x^{-1} but none of x, or exactly one occurrence of each of x and x^{-1}.

If G is $\mathbb{Z}_n$, with addition as the group operation, then x^{-1} in the above becomes $-x$, and the elements of the 2-sequencing are given by $b_1 = 0$ and $b_i = a_i - a_{i-1}$ $(i = 2, 3, \ldots, n)$.

Anderson and Preece [2] gave some general constructions for terraces for $\mathbb{Z}_n$ where n is an odd prime power, say $n = p^s$ with p an odd prime and s a positive integer. The terraces in [2] are *power-sequence terraces* in the sense that the constructions are based on sequences of powers of elements from $\mathbb{Z}_n$. Each such terrace can be partitioned into segments one of which contains merely the zero element. Each other segment is either (a) a sequence of successive powers of an element of $\mathbb{Z}_n$, or (b) such a sequence multiplied throughout by a constant. Here the phrase "successive powers" covers index-sequences of the form $i,\ \ i+\alpha,\ \ i+2\alpha, \ldots$, where α may be any suitable positive or negative integer. Anderson and Preece [3] provided further power-sequence terraces for $\mathbb{Z}_n$ with $n = p$. The terraces in [2,3] are based on powers of primitive roots for n, or of the negatives of such primitive roots, or of elements of order $(n-1)/2$, modulo n.

Anderson and Preece [4] moved on from prime-power values of n to construct certain power-sequence terraces for $\mathbb{Z}_n$ with $n = pq^t$ where p and q are distinct odd primes and t is a positive integer. This development required a move on from primitive roots of n to primitive λ-roots of n, as defined by Carmichael [7–9] and discussed in [6]. An example from [4] is the following power-sequence terrace for $\mathbb{Z}_{15}$:

$$3^4\ \ 3^5\ \mid\ 2^1\ \ 2^2\ \ 2^3\ \ 2^4\ \mid\ 5^2\ \mid\ 0\ \mid\ -5^2 \mid -2^4\ \ -2^3\ \ -2^2\ \ -2^1 \mid -3^5\ \ -3^4,$$

i.e.

$$6\quad 3\quad \mid\quad 2\quad 4\quad 8\quad 1\quad \mid\quad 10\quad \mid\quad 0\quad \mid\quad 5\quad \mid\quad 14\quad 7\quad 11\quad 13\quad \mid\quad 12\quad 9.$$

This terrace is based on the primitive λ-root 2 of 15; successive powers of the primitive λ-root appear in the second segment of the terrace. Here, as elsewhere, we omit brackets and commas from our notation for a terrace, and we use vertical bars, which we refer to as *fences*, to separate segments.

As the elements of the 2-sequencing for the terrace above are such that the set $\{b_2, b_3, \ldots, b_{(n+1)/2}\}$ is identical to $\{b_{(n+3)/2}, b_{(n+5)/2}, \ldots, b_n\}$, the terrace has the *half-and-half property* [1, p. 42]. Indeed, as it further has $b_i = b_{n+2-i}$ for all $i = 2, 3, \ldots, (n+1)/2$, it is *narcissistic* [2]. However, because of these properties, it has more segments than are needed for a power-sequence terrace for $\mathbb{Z}_{15}$. Two segments are indeed needed for the units of $\mathbb{Z}_{15}$ (i.e. for the non-zero elements of $\mathbb{Z}_{15}$ that are co-prime to 15), as the order of a primitive λ-root is the maximum order of a unit. However, we may hope to be able to put the non-zero multiples of 3, namely 3^1, 3^2, 3^3 and 3^4 (i.e. 3, 9, 12 and 6), into a single segment, as also the non-zero multiples of 5, namely 5^1 and 5^2 (i.e. 5 and 10). This hope is realised via Theorem 2.1. More generally, for $n = pq$ with p and q being distinct odd primes, this paper provides constructions for $\mathbb{Z}_n$ power-sequence terraces in which the number of segments is the lower bound $3 + \xi(n)$, where $\xi(n)$ is the ratio $\phi(n)/\lambda(n)$ of the number $\phi(n)$ of units in $\mathbb{Z}_n$ to the maximum order $\lambda(n)$ of a unit from $\mathbb{Z}_n$. The constructions, based on primitive λ-roots of *n*, have been developed so as to be fruitful in the range $n < 200$.

As in [4] (which gives details), a primitive λ-root of *n* is *negating* if it has -1 as a power, and *non-negating* otherwise. Likewise, a primitive λ-root *x* of *n* is *inward* if $x-1$ is a unit of $\mathbb{Z}_n$, and *outward* otherwise. A primitive λ-root that is non-negating and inward is *strong*. In all our constructions, the primitive λ-roots are inward, but they are not necessarily strong.

If the elements immediately before and after the *i*th fence ($i = 1, 2, \ldots$) are h_i and h'_i, respectively, we write $f_i = h'_i - h_i$ for the *fence difference* for the *i*th fence. If we write the *i*th *non-zero* segment ($i = 1, 2, \ldots$) in the form $|ag^j\, ag^{j+1} \ldots ag^{j+l}|$, we have $ag^{j+l+1} \equiv ag^j \pmod n$; for convenience in the present paper we write $m_i = ag^{j+l}(g-1)$ and we call m_i the *missing difference* for that segment. (When $n = 3p$, segments such as $|2p\;\; p|$ and $|2p\delta\;\; p\delta|$, as in Theorems 2.1 and 2.3, have $g = 2$.)

2. Terraces for $\mathbb{Z}_{3p}$

2.1. Terraces with zero in the third (middle) segment

Theorem 2.1. *Let p be an odd prime, $p \equiv 2 \pmod 3$, such that 2 is a strong primitive λ-root of $3p$. Let w be any primitive root of p, and choose α so that $w(w-1)^{-1} \equiv \pm 2^\alpha \pmod p$. Then choose β such that $2^{\alpha+1} \equiv -3w^\beta \pmod p$. Then*

$$2p \quad p \quad | \quad 2 \quad 4 \quad \ldots \quad 2^{p-2} \quad 1 \quad | \quad 0 \quad |$$
$$-2^\alpha \quad -2^{\alpha-1} \quad \ldots \quad -2^{\alpha+1} \quad | \quad 3w^\beta \quad 3w^{\beta+1} \quad \ldots \quad 3w^{\beta-1}$$

is a terrace for $\mathbb{Z}_{3p}$, with the units of $\mathbb{Z}_{3p}$ in the second and fourth segments.

Proof. The missing differences are $m_1 = p$, $m_2 = 1$, $m_3 = 2^\alpha$ and $m_4 = 3w^{\beta-1}(w-1)$. We show that the fence differences f_i $(i = 1, 2, 3, 4)$ compensate for these. Clearly, $f_2 = -1 = -m_2$ and $f_3 = -2^\alpha = -m_3$. For $f_1 = 2 - p$ we have $f_1 \equiv 0 \equiv m_4 \pmod 3$ and $m_4 \equiv \pm 3w^\beta 2^{-\alpha} \equiv \mp 2 \equiv \mp f_1 \pmod p$, so that $f_1 \equiv \pm m_4 \pmod{3p}$. Finally, $f_4 \equiv 2^{\alpha+1} \equiv \pm 1 \equiv \mp m_1 \pmod 3$, and $f_4 \equiv 0 \equiv m_1 \pmod p$, so that $f_4 \equiv \mp m_1 \pmod{3p}$. □

Note (a): As $\mathrm{ord}_{3p}(2) = p-1$, we have $\mathrm{ord}_p(2) = p-1$ or $(p-1)/2$. If $\mathrm{ord}_p(2) = p-1$, i.e. if 2 is a primitive root of *p*, then for any α, β chosen as above, $\alpha + (p-1)/2$, $\beta + (p-1)/2$ is another choice, the only change to the terrace being that the segments to the right of 0 are replaced by ones with the same cyclic order but starting half-way along. If $\mathrm{ord}_p(2) = (p-1)/2$, then replacing α by $\alpha + (p-1)/2$ changes the fourth segment as described above but the final segment is unchanged.

Note (b): If 2 is a primitive root of *p* we can always take $w = 2$ and $\alpha = 1$, and choose β so that $3 \times 2^{\beta-2} \equiv -1 \pmod p$; in the fourth segment of the terrace, the second element is then 1 greater than the first, as it must be whenever $\alpha = 1$. Also, if 2 is a primitive root of p we can always take $w = 2^{-1}$ and $\alpha = 0$, and choose β so that $2^{\beta+1} \equiv -3 \pmod p$; the fourth segment is then the reverse of the negative of the second segment.

Note (c): If, for given n, where $n = 3p$, the units w and $w(2w-1)^{-1}$ are both primitive roots of p, they provide terraces with the same value of α.

Note (d): In the range $n < 200$ Theorem 2.1 provides $\mathbb{Z}_n$ terraces for $n = 15, 69, 87, 141$ and 159 only, as 51 and 123 do not have 2 as a primitive λ-root, whereas 33 and 177 have 2 as a negating primitive λ-root.

Example 2.1(i). $p = 5, n = 15$.

Here 2 is a primitive root of p. The parameter sets yielding solutions are $(w, \alpha, \beta) = (2, 1, 1),\ (2, 3, 3),\ (3, 0, 0),\ (3, 2, 2)$. For the first of these the $\mathbb{Z}_{15}$ terrace is

$$10\ \ 5\ \ |\ \ 2\ \ 4\ \ 8\ \ 1\ \ |\ \ 0\ \ |\ \ 13\ \ 14\ \ 7\ \ 11\ \ |\ \ 6\ \ 12\ \ 9\ \ 3.$$

Example 2.1(ii). $p = 23, n = 69$.

Here 2 is not a primitive root of p. In ascending order for α, the parameter sets yielding solutions are

w	10	11	5	21	17	20	7	19	14	15
α	2	3	4	4	5	6	6	7	9	9
β	15	15	5	19	1	15	19	11	7	19

and a further 10 parameter sets obtained by adding 11 to the α-values in each of the above. The $\mathbb{Z}_{69}$ terrace for $(w, \alpha, \beta) = (20, 6, 15)$ is

$$46\ \ 23\ \ |\ \ 2\ \ 4\ \ \ldots\ \ 1\ \ |\ \ 0\ \ |\ \ 5\ \ 37\ \ \ldots\ \ 10\ \ |\ \ 33\ \ 39\ \ \ldots\ \ 12.$$

Example 2.1(iii). $p = 29, n = 87$.

Here 2 is a primitive root of p. In ascending order for α, the parameter sets yielding solutions are

w	2	11	26	3	18	8	21	14	27	10	19	15
α	1	2	3	4	4	5	7	9	10	13	12	0
β	11	24	11	14	14	5	1	23	20	1	18	18

and a further 12 parameter sets obtained by adding 14 to the α- and β-values in each of the above. The $\mathbb{Z}_{87}$ terrace for $(w, \alpha, \beta) = (2, 1, 11)$ is

$$58\ \ 29\ \ |\ \ 2\ \ 4\ \ \ldots\ \ 1\ \ |\ \ 0\ \ |\ \ 85\ \ 86\ \ 43\ \ \ldots\ \ 83\ \ |\ \ 54\ \ 21\ \ \ldots\ \ 27.$$

Theorem 2.2. *Let p be an odd prime,* $p \equiv 1 \pmod 3$, *such that* 2 *is a strong primitive* λ*-root of* $3p$. *Let* w *be any primitive root of p, and choose* α *so that* $w(w-1)^{-1} \equiv \pm 2^{\alpha} \pmod p$. *Then choose* β *such that* $2^{\alpha+1} \equiv -3w^{\beta} \pmod p$. *Then*

$$\begin{gathered} p\ \ 2p\ \ |\ \ 2\ \ 4\ \ \ldots\ \ 2^{p-2}\ \ 1\ \ |\ \ 0\ \ | \\ -2^{\alpha}\ \ -2^{\alpha-1}\ \ \ldots\ \ -2^{\alpha+1}\ \ |\ \ 3w^{\beta}\ \ 3w^{\beta+1}\ \ \ldots\ \ 3w^{\beta-1} \end{gathered}$$

is a terrace for $\mathbb{Z}_{3p}$, *with the units of* $\mathbb{Z}_{3p}$ *in the second and fourth segments.*

Proof. Exactly as for Theorem 2.1. □

Note (a): For each w there are two solutions, exactly as for Theorem 2.1. If 2 is a primitive root of p we can again take $w = 2$ and $\alpha = 1$, or take $w = 2^{-1}$ and $\alpha = 0$.

Note (b): In the range $n < 200$, where $n = 3p$, Theorem 2.2 provides $\mathbb{Z}_n$ terraces for $n = 21$, 39, 111 and 183 only, as 57 has 2 as a negating primitive λ-root, whereas 93 and 129 do not have 2 as a primitive λ-root.

Example 2.2(i). $p = 7$, $n = 21$.

Here 2 is not a primitive root of p. The parameter sets providing solutions are $(w, \alpha, \beta) = (3, 1, 0)$, $(3, 4, 0)$, $(5, 2, 4)$ and $(5, 5, 4)$. For the first of these the $\mathbb{Z}_{21}$ terrace is

$$7 \;\; 14 \;\mid\; 2 \;\; 4 \;\; \ldots \;\; 1 \;\mid\; 0 \;\mid\; 19 \;\; 20 \;\; 10 \;\; \ldots \;\; 17 \;\mid\; 3 \;\; 9 \;\; \ldots \;\; 15.$$

Example 2.2(ii). $p = 13$, $n = 39$.

Here 2 is a primitive root of p. The parameter sets providing solutions are $(w, \alpha, \beta) = (2, 1, 4)$, $(6, 2, 1)$, $(7, 0, 3)$ and $(11, 3, 6)$, and the further 4 solutions obtained by adding 6 to the α- and β-values in each of the above. The $\mathbb{Z}_{39}$ terrace for $(w, \alpha, \beta) = (2, 1, 4)$ is

$$13 \;\; 26 \;\mid\; 2 \;\; 4 \;\; \ldots \;\; 1 \;\mid\; 0 \;\mid\; 37 \;\; 38 \;\; 19 \;\; \ldots \;\; 35 \;\mid\; 9 \;\; 18 \;\; \ldots \;\; 24.$$

Theorem 2.3. *Let p be a prime, $p \equiv 3 \pmod 4$, $p > 3$, for which 2 is a primitive root, so that 2 is a negating primitive λ-root of $3p$. Let w be any primitive root of p. Choose $\delta = 1$ or 2 so that $p\delta \equiv 2 \pmod 3$. Take a to be a non-multiple of 3 satisfying $a \equiv w(w-1)^{-1} \pmod p$ and $a \notin S_2$ where $S_2 = \{1, 2, \ldots, 2^{p-2}\}$. Take b to be whichever of $2a + p$ and $2a + 2p$ is a multiple of 3. Then*

$$2p\delta \;\; p\delta \;\mid\; 2 \;\; 4 \;\; \ldots \;\; 1 \;\mid\; 0 \;\mid\; a \;\; 2^{p-2}a \;\; 2^{p-3}a \;\; \ldots \;\; 2a \;\mid\; b \;\; bw \;\; \ldots \;\; bw^{p-2}$$

is a $\mathbb{Z}_{3p}$ terrace with the units of $\mathbb{Z}_{3p}$ in the second and fourth segments.

Proof. Very similar to the proof of Theorem 2.1. $\square$

Note (a): For $n < 200$, where $n = 3p$, Theorem 2.3 yields $\mathbb{Z}_n$ terraces for only $n = 33$, 57 and 177, but these values of n are not covered by either Theorem 2.1 or Theorem 2.2.

Note (b): A special case of Theorem 2.3 is obtained by taking $w = 2$, $a = \delta p + 2$ and $b = \delta p + 4$.

Example 2.3. $p = 19$, $n = 57$.

We can use $(w, a, b, \delta) = (2, 40, 42, 2)$ to obtain the $\mathbb{Z}_{57}$ terrace

$$19 \;\; 38 \;\mid\; 2 \;\; 4 \;\; \ldots \;\; 1 \;\mid\; 0 \;\mid\; 40 \;\; 20 \;\; \ldots \;\; 23 \;\mid\; 42 \;\; 27 \;\; \ldots \;\; 21.$$

Other than 2, there are five primitive roots of p, namely 3, 10, 13, 14 and 15. Using $(w, a, b, \delta) = (3, 11, 3, 2)$ we obtain the $\mathbb{Z}_{57}$ terrace

$$19 \;\; 38 \;\mid\; 2 \;\; 4 \;\; \ldots \;\; 1 \;\mid\; 0 \;\mid\; 11 \;\; 34 \;\; \ldots \;\; 22 \;\mid\; 3 \;\; 9 \;\; \ldots \;\; 39.$$

Theorem 2.4. *Let p be an odd prime such that 2 is a primitive root of p and a primitive λ-root of $3p$. Choose $\delta = 1$ or 2 so that $\delta p \equiv 2 \pmod 3$. Write $a \equiv 2\delta p + 1$ and*

$b \equiv 4\delta p + 1 \pmod{3p}$. *Then the sequences*

$$a \;\; 2^{p-2}a \;\; 2^{p-3}a \;\; \ldots \;\; 2^1 a \;\mid\; b \;\; 2^1 b \;\; 2^2 b \;\; \ldots \;\; 2^{p-2}b \;\mid$$
$$0 \;\mid\; 2\delta p \;\; \delta p \;\mid\; 1 \;\; 2^{p-2} \;\; 2^{p-3} \;\; \ldots \;\; 2^1$$

and

$$2^1 a \;\; 2^2 a \;\; \ldots \;\; 2^{p-2}a \;\; a \;\mid\; 2^1 b \;\; 2^2 b \;\; \ldots \;\; 2^{p-2}b \;\; b \;\mid$$
$$0 \;\mid\; 2\delta p \;\; \delta p \;\mid\; 1 \;\; 2^{p-2} \;\; 2^{p-3} \;\; \ldots \;\; 2^1$$

are terraces for $\mathbb{Z}_{3p}$, each having the units of $\mathbb{Z}_{3p}$ in the first and last segments. If $p \equiv 3 \pmod 4$, then 2 is a negating primitive λ-root of $3p$, and each sequence remains a terrace if its first two segments are multiplied throughout by -1.

Proof. Almost immediate. The unit a, as defined, cannot be in S_2 as $1 \in S_2$ and all entries in S_2 are incongruent modulo p. $\square$

Note: In the range $n < 200$, where $n = 3p$, Theorem 2.4 provides $\mathbb{Z}_n$ terraces for $n = 15, 39, 87, 111, 159, 183$ (all with $p \equiv 1$, mod 4) and for $n = 33, 57, 177$ (all with $p \equiv 3$, mod 4).

Example 2.4. $p = 11, n = 33$.

Use $(a, b, \delta) = (23, 12, 1)$ in the first sequence in Theorem 2.4 to give the $\mathbb{Z}_{33}$ terrace

$$23 \;\; 28 \;\; \ldots \;\; 13 \;\mid\; 12 \;\; 24 \;\; \ldots \;\; 6 \;\mid\; 0 \;\mid\; 22 \;\; 11 \;\mid\; 1 \;\; 17 \;\; \ldots \;\; 2.$$

2.2. Terraces with zero in the first segment

Theorem 2.5. *Let p be any prime, $p \geqslant 5$. Suppose that x, given by $2x \equiv 3 \pmod p$, is a primitive root of p with $x \equiv 2 \pmod 3$. Define a by $9a \equiv 4 \pmod p$ and $a \equiv 2 \pmod 3$. Then $a \notin S_x$ where S_x is the subset $S_x = \{1, x, x^2, \ldots, x^{p-2}\}$ of elements of $\mathbb{Z}_{3p}$. Take $\delta = 1$ or 2 so that $\delta p \equiv 2 \pmod 3$. Then*

$$0 \;\mid\; 2\delta p \;\; \delta p \;\mid\; a \;\; ax^{p-2} \;\; ax^{p-3} \;\; \ldots \;\; ax \;\mid$$
$$3x^{p-4} \;\; 3x^{p-5} \;\; \ldots \;\; 3x^{-2} \;\mid\; x^0 \;\; x^1 \;\; \ldots \;\; x^{p-2}$$

is a $\mathbb{Z}_{3p}$ terrace with the units of $\mathbb{Z}_{3p}$ in the third and fifth segments.

Proof. We first show that $a \notin S_x$. Suppose that $a = x^i$. Then $2^i \equiv 2 \pmod 3$ so that i is odd. But $ax^2 \equiv 1 \pmod p$, so $x^{i+2} \equiv 1 \pmod p$, which requires i to be even, giving us a contradiction. As a is clearly a unit, the set of units of $\mathbb{Z}_{3p}$ can thus be written as $S_x \cup aS_x$.

Trivially, $m_1 = \pm p = -f_1$.

Next, $m_2 = a(1-x)$ and $f_3 = 3x^{p-4} - ax$. Thus $m_2 = -f_3$ as, modulo 3, we have $m_2 \equiv -a \equiv 2a \equiv -f_3$ and, modulo p, we have $-m_2 \equiv x^{-2}(x-1) \equiv x^{-2}(2x-1) - x^{-1} \equiv 3x^{p-4} - ax \equiv f_3$.

Next, $m_3 = 3x^{p-4}(1-x)$ and $f_2 = a - \delta p$. Thus $m_3 = -f_2$ as, modulo 3, we have $m_3 \equiv 0 \equiv f_2$ and, modulo p, we have $m_3 \equiv x^{-2}(2x-1)(x-1) \equiv \frac{4}{9} \times 2 \times \frac{1}{2} \equiv \frac{4}{9} \equiv x^{-2} \equiv a \equiv f_2$.

Then, $m_4 = x^{p-2}(x-1)$ and $f_4 = 1 - 3x^{p-3}$. Thus $m_4 = -f_4$ as, modulo 3, we have $m_4 \equiv 2^{p-2} \equiv -1 \equiv -f_4$ and, modulo p, we have $m_4 \equiv x^{-1}(x-1) \equiv x^{-1}(3x^{p-2} - x) \equiv 3x^{p-3} - 1 \equiv -f_4$.

The differences arising from the proposed terrace are therefore $\pm p$, $\pm 2p$, $a(x-1)x^i$, $(x-1)x^i$, $3(x-1)x^i$ for $0 \leqslant i \leqslant p-2$. As $\gcd(x-1, 3p) = 1$, these differences are precisely the elements of $S_x \cup aS_x \cup (3\mathbb{Z}_p \backslash \{0\})$, i.e. of $\mathbb{Z}_{3p} \backslash \{0\}$. □

Note (a): As $x \equiv 2 \pmod 3$, we have $\mathrm{ord}_{3p}(x) = \mathrm{lcm}(p-1, 2) = p-1$, so x is an inward primitive λ-root of $3p$. If $p \equiv 3 \pmod 4$ then x is a negating primitive λ-root, but it is a strong primitive λ-root if $p \equiv 1 \pmod 4$.

Note (b): In the range $n < 200$, where $n = 3p$, Theorem 2.5 provides $\mathbb{Z}_n$ terraces for $n = 21, 33, 51, 93, 111, 123$ and 177. The values of the parameters for these terraces are as in the Note following Theorem 2.6.

Example 2.5. $p = 11$, $n = 33$.

Use $(x, a, \delta) = (29, 20, 1)$ to obtain the $\mathbb{Z}_{33}$ terrace

$$0 \mid 22 \;\; 11 \mid 20 \;\; 28 \;\; \ldots \;\; 19 \mid 18 \;\; 12 \;\; \ldots \;\; 27 \mid 1 \;\; 29 \;\; \ldots \;\; 8.$$

Theorem 2.6. *Let p be any prime,* $p \geqslant 5$. *Suppose that x, given by* $2x \equiv 3 \pmod p$, *is a primitive root of p with* $x \equiv 2 \pmod 3$. *Define a by* $a \equiv 1 \pmod 3$ *and* $6a \equiv 1 \pmod p$. *Then* $a \notin S_x$ *where* S_x *is as in Theorem* 2.5. *Take* $\delta = 1$ *or* 2 *so that* $\delta p \equiv 1 \pmod 3$, *and define b by* $b \equiv (2-x)x^{-1} \pmod{3p}$, *so that* $b \equiv 3^{-1} \pmod p$ *and* $3|b$. *Then*

$$0 \mid 2\delta p \;\; \delta p \mid a \;\; ax^{p-2} \;\; ax^{p-3} \;\; \ldots \;\; ax \mid$$
$$b \;\; bx^{p-2} \;\; bx^{p-3} \;\; \ldots \;\; bx \mid x^0 \;\; x^{p-2} \;\; x^{p-3} \;\; \ldots \;\; x$$

is a $\mathbb{Z}_{3p}$ *terrace with the units of* $\mathbb{Z}_{3p}$ *in the third and fifth segments.*

Proof. Similar to that of Theorem 2.5. □

Note: Theorems 2.5 and 2.6 provide $\mathbb{Z}_n$ terraces for the same values of n, where $n = 3p$. For each such n, the two theorems have the same inward primitive λ-root x of n but a different value of δ. The values taken by the parameters for the terraces from Theorems 2.5 and 2.6 are as follows, where negating primitive λ-roots are marked $^{\mathrm{neg}}$:

n	p	x	Theorem 2.5		Theorem 2.6		
			a	δ	a	b	δ
21	7	5^{neg}	2	2	13	12	1
33	11	29^{neg}	20	1	13	15	2
51	17	44	8	1	37	6	2
93	31	17^{neg}	59	2	88	21	1
111	37	20	95	2	31	99	1
123	41	104	5	1	7	96	2
177	59	149^{neg}	125	1	10	138	2

Example 2.6. $p = 11$, $n = 33$.

Use $(x, a, b, \delta) = (29, 13, 15, 2)$ to obtain the $\mathbb{Z}_{33}$ terrace

$$0 \;|\; 11 \;\; 22 \;|\; 13 \;\; 5 \;\; \ldots \;\; 14 \;|\; 15 \;\; 21 \;\; \ldots \;\; 6 \;|\; 1 \;\; 8 \;\; \ldots \;\; 29.$$

Theorem 2.7. *Let p be a prime, $p \geqslant 7$, and let $\delta = 1$ or 2 according as $p \equiv 2$ or $1 \pmod 3$. Let x be a primitive λ-root of $3p$ such that $x \equiv 2 \pmod 3$ and $1 - x$ is not a square modulo p. Let $a = (\delta p - 1)x(x-1)^{-1}$. Then $a \equiv 2 \pmod 3$ and $a \notin S_x$ where S_x is as in Theorem 2.5. Suppose that y, given by $y \equiv 1 \pm (x^2 + x - 1)(x^2 - 3x + 1)^{-1} \pmod p$, is a primitive root of p. Then, for a value b chosen to be a multiple of 3 that satisfies $b \equiv (x + a - 1)x^{-1} \pmod{3p}$, the sequence*

$$0 \;|\; 2\delta p \;\; \delta p \;|\; 1 \;\; x \;\; \ldots \;\; x^{p-2} \;|\; a \;\; ax \;\; \ldots \;\; ax^{p-2} \;|\; b \;\; by^{-1} \;\; \ldots \;\; by^{-(p-2)}$$

is a $\mathbb{Z}_{3p}$ terrace with the units of $\mathbb{Z}_{3p}$ in the third and fourth segments.

Proof. We have $\delta p - 1 \equiv 1 \pmod 3$, so $a \equiv 2 \pmod 3$; also $a \equiv -x(x-1)^{-1} \pmod p$. Suppose $a \in S_x$, say $a \equiv x^i \pmod{3p}$. Then $2 \equiv 2^i \pmod 3$ so that i is odd. Also, $x^i \equiv -x(x-1)^{-1} \pmod p$, so $1 - x \equiv x^{1-i} \pmod p$. But $1 - x$ is not a square, so i must be even, giving a contradiction. So $a \notin S_x$.

We have $m_1 = \pm p$, $m_2 = 1 - x^{-1}$, $m_3 = a(1 - x^{-1})$ and $m_4 = b(1 - y)$. Also $f_1 = \pm p$, $f_2 = 1 - \delta p$, $f_3 = a - x^{-1}$ and $f_4 = b - ax^{-1}$. Clearly, $m_1 = \pm f_1$, and the choice of a gives us $m_3 = -f_2$. For $m_2 = f_4$ we need $(x-1)x^{-1} = b - ax^{-1}$, i.e.

$$b \equiv (x + a - 1)x^{-1} \pmod{3p}, \tag{1}$$

and for $m_4 = \pm f_3$ we need

$$b(y - 1) \equiv \pm(a - x^{-1}) \pmod{3p}. \tag{2}$$

The congruence $a \equiv 2 \pmod 3$ implies that (1) and (2) are automatically satisfied (mod 3). Now (1) and (2) are equivalent to (1) and the congruence $(x + a - 1)x^{-1}(y - 1) \equiv \pm(ax - 1)x^{-1} \pmod p$, i.e.

$$y \equiv 1 \pm (ax - 1)(x + a - 1)^{-1} \pmod p. \tag{3}$$

So if y, given by (3), is a primitive root of p, we can use (1) to determine b. □

Note (a): We can always find a primitive root x of p for which $1 - x$ is, modulo p, a non-square [10, p. 146]. So an appropriate primitive λ-root x always exists, and the success of the construction depends only on y being a primitive root. In the range $n < 200$, Theorem 2.7 produces $\mathbb{Z}_n$ terraces with $n = 3p$ for all prime p satisfying $p \geqslant 7$ except for $p = 13$. We have, however, no proof that 13 is the only p-value for which the theorem fails. For some values of p, both of the values of y satisfying (3) for a particular x are primitive roots; either can then be used to provide a terrace.

Note (b): If $n = 3p$ where p is a prime satisfying $p \equiv 11 \pmod{12}$ and 2 is a primitive λ-root of n, then Theorem 2.7 produces $\mathbb{Z}_n$ terraces with $(n, x, a, y, b) = (3p,\ 2,\ 2(p - 1),\ p - 4,\ (5p - 1)/2)$. This is because, for the values of p under consideration, $p - 4$ is always a primitive root of p, and the a-value $2(p - 1)$ is not a power of 2. With $x = 2$ and $a = 2(p - 1)$, the alternative y-value obtainable from (3) is 6; whether this is a primitive root of p is a question having no easy general answer.

Note (c): If $n = 3p$ where p is a prime satisfying $p \equiv 7 \pmod{12}$ and 2 is a primitive λ-root of n, then Theorem 2.7 produces $\mathbb{Z}_n$ terraces with $(n, x, a, y, b) = (3p,\ 2,\ p - 2,\ p - 4,\ (p - 1)/2)$. Again, for the values of p under consideration, $p - 4$ is always a primitive root of p, but 6 may or may not be a primitive root of p.

Note (d): We clearly cannot ever have $a = -1$ in Theorem 2.7. However, a special case of this theorem sometimes produces terraces with $a = 2$. If $a = 2$, the relationship $-x(x - 1)^{-1} \equiv a \pmod p$ yields $3x \equiv 2 \pmod p$. But then the value $1 - x = 3^{-1}$ must not be a square (mod p), whence 3 must not be a square (mod p). Thus $p \equiv 5$ or $7 \pmod{12}$. So $p \equiv 5$ or 7 or 17 or $19 \pmod{24}$. We now rule out $p \equiv 5 \pmod{24}$.

Let $p \equiv 5 \pmod{24}$ and suppose that $-2 \in S_x$. Then $-2 \equiv x^i \pmod{3p}$ for some i. Thus $2^i \equiv 1 \pmod 3$, whence i is even. So -2 is a square, modulo p, which gives us a contradiction if $p \equiv 5 \pmod 8$. Thus $-2 \notin S_x$. As x is non-negating, we have $2 \in S_x$, so we cannot take $a = 2$.

Accordingly, the value $a = 2$ can arise only if $p \equiv 17 \pmod{24}$ or $p \equiv 7 \pmod{12}$. In the first case x must be a primitive root of p and a strong primitive λ-root of n; in the second case x can be strong ($^{\mathrm{strg}}$) or negating ($^{\mathrm{neg}}$). In the range $n < 200$, the $\mathbb{Z}_n$ terraces with $n = 3p$ and $a = 2$ that are obtainable from the theorem are given by $(n,\ p, x, a,\ y,\ b) = (21, 7, 17^{\mathrm{neg}}, 2, 5, 6)$, $(51, 17, 29, 2, 11, 45)$, $(123, 41, 110, 2, 34, 105)$ and $(129, 43, 101^{\mathrm{strg}}, 2, 18, 24)$. The absence of such a terrace for $n = 93$ is entirely due to the lack of a suitable primitive root y.

For $n = 129$, the value $x = 101$ (with $a = 2$) is the only strong primitive λ-root that yields a terrace obtainable from Theorem 2.7.

Note (e): For $n < 200$, sets of parameter values for $\mathbb{Z}_n$ terraces obtainable from Theorem 2.7 are as in the following table, where † indicates a p-value satisfying $p \equiv 3 \pmod 4$, so that x may be a strong ($^{\mathrm{strg}}$) or negating ($^{\mathrm{neg}}$) primitive λ-root. In each line of the table, the parameter set listed is not in general the only one available.

n	p	x	a	y	b	Note
21	$7^{\dagger}$	2^{strg}	5	3	3	(c)
		5^{neg}	11	3	3	
33	$11^{\dagger}$	26^{strg}	17	7 or 6	27	
		2^{neg}	20	7 or 6	27	(b)
39	13	—	—	—	—	(a)
51	17	23	26	6	42	
57	$19^{\dagger}$	17^{strg}	50	13	24	
		2^{neg}	17	15	9	(c)
69	$23^{\dagger}$	2^{strg}	44	19	57	(b)
		17^{neg}	32	17	15	
87	29	11	83	8	48	
93	$31^{\dagger}$	41^{strg}	23	13	90	
		65^{neg}	14	12 or 21	57	(d)
111	37	20	71	18	60	
123	41	29	59	15 or 28	3	
129	$43^{\dagger}$	101^{strg}	2	18	24	(d)
		26^{neg}	11	34	51	
141	$47^{\dagger}$	2^{strg}	92	43	117	(b)
		23^{neg}	125	10 or 39	129	
159	53	20	38	45	138	
177	$59^{\dagger}$	5^{strg}	161	52	33	
		2^{neg}	116	55 or 6	147	(b)
183	61	44	77	17	36	

Example 2.7(i). $p = 7, n = 21$.
Use $(x, a, y, b) = (5, 11, 3, 3)$ to obtain the $\mathbb{Z}_{21}$ terrace

$$0 \mid 7 \ 14 \mid 1 \ 5 \ 4 \ 20 \ 16 \ 17 \mid 11 \ 13 \ 2 \ 10 \ 8 \ 19 \mid 3 \ 15 \ 12 \ 18 \ 6 \ 9.$$

Example 2.7(ii). $p = 11, n = 33$.
Use $(x, a, y, b) = (2, 20, 7, 27)$ to obtain the $\mathbb{Z}_{33}$ terrace

$$0 \mid 22 \ 11 \mid 1 \ 2 \ 4 \ \ldots \ 17 \mid 20 \ 7 \ 14 \ \ldots \ 10 \mid 27 \ 18 \ 12 \ \ldots \ 24.$$

2.3. Terraces with zero in the second segment

Theorem 2.8. *Let p be an odd prime having 2 as a primitive root. Let x be a primitive λ-root of $3p$ such that $x \equiv 2 \pmod 3$. Write $a = (1 - x)^{-1}$ and $b = (1 - x)^{-1} - x^{-1}$.*

Then $a \equiv 2 \pmod 3$ *and* $3|b$. *If* $a \notin S_x$, *the sequence*

$$p \quad 2p \quad | \quad 0 \quad | \quad 1 \quad x \quad x^2 \quad \ldots \quad x^{p-2} \quad |$$
$$a \quad ax^{p-2} \quad ax^{p-3} \quad \ldots \quad ax \quad | \quad b \quad 2^{p-2}b \quad 2^{p-3}b \quad \ldots \quad 2b$$

is a $\mathbb{Z}_{3p}$ *terrace with the units of* $\mathbb{Z}_{3p}$ *in the third and fourth segments.*

Proof. Straightforward. □

Note (a): In any terrace obtainable from this or the next theorem, the elements in the first segment can of course be interchanged.

Note (b): If, in addition to the conditions of Theorem 2.8, we have $p \equiv 1 \pmod 4$, then 2 is a strong primitive λ-root of $3p$, so we can take $x = 2$. Then $a = -1$ and $b = -3 \times 2^{p-2} = 3(p-1)/2$.

Note (c): In the range $n < 200$, where $n = 3p$, Theorem 2.8 produces $\mathbb{Z}_n$ terraces for the values of n in the following table, which gives specimen parameter sets:

n	p	(x, a, b)		
		$x = 2$, strong	x strong, $\neq 2$	x negating, $\neq 2$
15	5	(2, 14, 6)	—	—
33	11	—	(5, 8, 21)	(8, 14, 18)
39	13	(2, 38, 18)	(11, 35, 3)	—
57	19	—	(5, 14, 48)	(14, 35, 39)
87	29	(2, 86, 42)	(8, 62, 51)	—
111	37	(2, 110, 54)	(5, 83, 105)	—
159	53	(2, 158, 78)	(8, 68, 48)	—
177	59	—	(5, 44, 150)	(11, 53, 69)
183	61	(2, 182, 90)	(35, 113, 45)	—

Example 2.8. $p = 5$, $n = 15$. We have the $\mathbb{Z}_{15}$ terrace

$$5 \quad 10 \quad | \quad 0 \quad | \quad 1 \quad 2 \quad 4 \quad 8 \quad | \quad 14 \quad 7 \quad 11 \quad 13 \quad | \quad 6 \quad 3 \quad 9 \quad 12.$$

Theorem 2.9. *Let p be an odd prime such that* 2 *is a primitive* λ*-root of* $3p$. *Let* w *be any primitive root of p. Suppose that there is a unit a satisfying* $a \equiv 2 \pmod 3$, $a \notin S_2$ *where* S_2 *is as in Theorem* 2.4, *and either*

$$a \equiv 2w(4w-3)^{-1} \pmod p \tag{4}$$

or

$$a \equiv -2w(2w-3)^{-1} \pmod p. \tag{5}$$

Then

$$p \quad 2p \quad | \quad 0 \quad | \quad 1 \quad 2^{p-2} \quad 2^{p-3} \quad \dots \quad 2^1 \quad | \quad a \quad 2^{p-2}a \quad 2^{p-3}a \quad \dots \quad 2a \quad |$$
$$3a \quad 3wa \quad \dots \quad 3w^{p-2}a$$

is a $\mathbb{Z}_{3p}$ *terrace with the units of* $\mathbb{Z}_{3p}$ *in the third and fourth segments*.

Proof. Straightforward. □

Note (a): If we take $w=2$ in Theorem 2.9, then (4) and (5), respectively, yield $a \equiv 4 \times 5^{-1} \pmod p$ and $a \equiv -4 \pmod p$. The latter, in conjunction with the congruence $a \equiv 2 \pmod 3$, yields $a \equiv -4 \pmod{3p}$, which is always admissible if $p \equiv 1 \pmod 4$, as we then have $-4 \notin S_2$, but is inadmissible if $p \equiv 3 \pmod 4$, as 2 is then a negating primitive λ-root of $3p$. If we take $w = 2^{-1}$ in Theorem 2.9, (4) and (5), respectively, yield $a \equiv -1 \pmod p$ and $a \equiv 2^{-1} \pmod p$. The former yields terraces with $a \equiv -1 \pmod{3p}$ if $p \equiv 1 \pmod 4$, but the latter is inadmissible as, modulo $3p$, we have $2^{-1} \in S_2$.

Note (b): If $p \equiv 1 \pmod 4$, then we can take $w \equiv -2$ or $w = -2^{-1}$ in Theorem 2.9. The latter, in conjunction with (5), yields $a \equiv -2^{p-3}$, which produces further terraces of a particularly simple form.

Note (c): The other simple special case arises when we can take $w=3$. Then (5) becomes $a \equiv -2 \pmod p$. This yields, for example, a $\mathbb{Z}_{21}$ terrace with $a=5$.

Note (d): In the range $n < 200$, where $n = 3p$, Theorem 2.9 covers the n-values listed in the following table, which provides specimen parameter sets for $\mathbb{Z}_n$ terraces obtainable from the theorem:

n	15	21	33	39	57	69	87	111	141	159	177	183
p	5	7	11	13	19	23	29	37	47	53	59	61
w	2	3	2	2	2	5	2	2	5	2	2	2
a (from (4))	—	17	14	—	35	29	53	—	125	—	107	74
a (from (5))	11	5	—	35	—	38	83	107	—	155	—	179

Note (e): Theorem 2.9 can be generalised by replacing every 2 in the fourth segment of the terrace by x, and every 3 in the fifth segment by $2x-1$, where x is a primitive λ-root of $3p$ with $x \in S_2$ and $x \equiv 2 \pmod 3$. However, even the generalisation is a special case (in different notation) of Theorem 3.7 below, so we omit details here.

Example 2.9. $p=7$, $n=21$.

Use $(w, a) = (3, 17)$ to obtain the $\mathbb{Z}_{21}$ terrace

$$7 \quad 14 \quad | \quad 0 \quad | \quad 1 \quad 11 \quad 16 \quad 8 \quad 4 \quad 2 \quad | \quad 17 \quad 19 \quad 20 \quad 10 \quad 5 \quad 13 \quad | \quad 9 \quad 6 \quad 18 \quad 12 \quad 15 \quad 3,$$

or use $(w, a) = (3, 5)$ to obtain

$$7 \quad 14 \quad | \quad 0 \quad | \quad 1 \quad 11 \quad 16 \quad 8 \quad 4 \quad 2 \quad | \quad 5 \quad 13 \quad 17 \quad 19 \quad 20 \quad 10 \quad | \quad 15 \quad 3 \quad 9 \quad 6 \quad 18 \quad 12.$$

3. Terraces for $\mathbb{Z}_{pq}$ with $\xi(pq) = 2$

3.1. Terraces with zero in the third segment

We now introduce Theorem 3.1 as a generalisation of Theorems 2.1 and 2.2 to the case in which $n = pq$ where p and q are distinct odd primes satisfying $\gcd(p-1, q-1) = 2$, so that $\xi(n) = 2$.

Theorem 3.1. *Let $n = pq$ where p and q are distinct odd primes satisfying* $\gcd(p-1, q-1) = 2$. *Suppose that* 2 *is a primitive root of q and a strong primitive λ-root of n, so that* $\mathrm{ord}_n(2) = (p-1)(q-1)/2$ *and thus so that* $\mathrm{ord}_p(2)$ *is* $(p-1)$ *or* $(p-1)/2$. *Choose δ so that* $\delta p \equiv 2 \pmod q$ *and let w be any primitive root of p. Choose α so that* $w(w-1)^{-1} \equiv \pm 2^\alpha \pmod p$ *and* $\alpha \equiv (q-3)/2 \pmod{(q-1)/2}$. *Choose b to satisfy $q|b$ and* $2^{\alpha+1} \equiv -b \pmod p$. *Then*

$$2^{q-2}\delta p \;\; 2^{q-3}\delta p \;\; \ldots \;\; 2^0\delta p \;|\; 2 \;\; 4 \;\; \ldots \;\; 1 \;|\; 0 \;|$$
$$-2^\alpha \;\; -2^{\alpha-1} \;\; \ldots \;\; -2^{\alpha+1} \;|\; b \;\; bw \;\; \ldots \;\; bw^{p-2}$$

is a $\mathbb{Z}_n$ terrace with the units of $\mathbb{Z}_n$ in the second and fourth segments of the terrace.

Proof. Trivially, $m_2 = 1 = -f_2$ and $m_3 = 2^\alpha = -f_3$.

Next, $m_1 = -2^{q-2}\delta p$ and $f_4 = b + 2^{\alpha+1}$. Thus $m_1 = \pm f_4$ as, modulo p, we have $m_1 \equiv 0 \equiv f_4$ and, modulo q, we have, for some integer μ, $f_4 \equiv 2^{\alpha+1} \equiv 2^{\mu(q-1)/2} \equiv \pm 1 \equiv \pm 2^{q-1} \equiv \pm 2^{q-2}\delta p \equiv \mp m_1$.

Finally, $m_4 = bw^{-1}(w-1)$ and $f_1 = 2 - \delta p$. Thus $m_4 = \pm f_1$ as, modulo p, we have $m_4 \equiv b(w-1)w^{-1} \equiv \pm 2^{\alpha+1} \times 2^{-\alpha} \equiv \pm 2 \equiv \pm f_1$ and, modulo q, we have $m_4 \equiv 0 \equiv f_1$. $\square$

Note (a): If $q = 5$, and 2 is a primitive root of p as well as of q, we can always take $w = 2$ and $\alpha = 1$, and choose b to be the multiple of q that satisfies $b \equiv -4 \pmod p$.

Note (b): As for Theorems 2.1 and 2.2, if w and $w(2w-1)^{-1}$ are both primitive roots of p, then they provide terraces with the same value of α.

Note (c): For $n < 200$ with $p, q > 3$, sets of parameter values for terraces obtainable from Theorem 3.1 are as follows:

n	p	q	w	δ	α	b	Note
35	7	5	3	1	1	10	
55	5	11	2	7	9	11	
	11	5	2	2	1	40	(a)
77	7	11	3	5	4	66	
95	5	19	2	8	17	76	
	19	5	2	3	1	15	(a)
115	23	5	7	4	1	65	
143	11	13	2	12	11	117	
	13	11	2	1	19	121	

Example 3.1. $(n, p, q) = (55, 5, 11)$.
Use $(w, \delta, \alpha, b) = (2, 7, 9, 11)$ to give the $\mathbb{Z}_{55}$ terrace

$$45\ \ 50\ \ \ldots\ \ 35\ \mid\ 2\ \ 4\ \ \ldots\ \ 1\ \mid\ 0\ \mid\ 38\ \ 19\ \ \ldots\ \ 21\ \mid\ 11\ \ 22\ \ 44\ \ 33.$$

Theorem 3.2. *Let $n = pq$ where p and q are distinct odd primes satisfying $\gcd(p-1, q-1) = 2$ and $q \equiv 3 \pmod 4$. Suppose that 2 is a strong primitive λ-root of n and that $\operatorname{ord}_q(2) = (q-1)/2$. Choose δ so that $\delta p \equiv 2 \pmod q$ and let w be any primitive root of p. Choose α so that $w(w-1)^{-1} \equiv \pm 2^{\alpha} \pmod p$ and so that $2^{\alpha+1} \equiv \pm 3 \pmod q$. Choose b to satisfy $q|b$ and $2^{\alpha+1} \equiv -b \pmod p$. Then*

$$(-2)^{q-2}\delta p\ \ (-2)^{q-3}\delta p\ \ \ldots\ \ (-2)^{0}\delta p\ \mid\ 2\ \ 4\ \ \ldots\ \ 1\ \mid\ 0\ \mid$$
$$-2^{\alpha}\ \ -2^{\alpha-1}\ \ \ldots\ \ -2^{\alpha+1}\ \mid\ b\ \ bw\ \ \ldots\ \ bw^{p-2}$$

is a $\mathbb{Z}_n$ terrace with the units of $\mathbb{Z}_n$ in the second and fourth segments of the terrace.

Proof. Similar to that for Theorem 3.1. As $\operatorname{ord}_q(2) = (q-1)/2$, the value -2 is a primitive root of q, so that $(-2)^{\alpha+1} \equiv 3 \pmod q$ for some α. Thus we can always find a suitable value of α for the terrace. □

Note: In the range $n < 200$ with $p, q > 3$, Theorem 3.2 provides solutions for $(n, p, q) = (35, 5, 7)$ and $(77, 11, 7)$ only. For $(n, p, q, \delta) = (35, 5, 7, 6)$ we have the parameter sets $(w, \alpha, b) = (2, 1, 21)$ and $(3, 10, 7)$ and two further possibilities obtained from these by adding 6 to α and negating b. For $(n, p, q, \delta) = (77, 11, 7, 4)$ we have $(w, \alpha, b) = (2, 1, 7)$, $(6, 10, 42)$, $(7, 13, 28)$ and $(8, 1, 7)$ and four further possibilities obtained from these by adding 15 to α and negating b.

Example 3.2. $(n, p, q) = (35, 5, 7)$.
Use $(w, \delta, \alpha, b) = (2, 6, 1, 21)$ to give the $\mathbb{Z}_{35}$ terrace

$$20\ \ 25\ \ \ldots\ \ 30\ \mid\ 2\ \ 4\ \ \ldots\ \ 1\ \mid\ 0\ \mid\ 33\ \ 34\ \ 17\ \ \ldots\ \ 31\ \mid\ 21\ \ 7\ \ 14\ \ 28.$$

Theorem 3.3. *Let $n = pq$ where p and q are odd primes, $p \equiv 5 \pmod 8$ and $q \equiv 3 \pmod 8$, such that $\gcd(p-1, q-1) = 2$, with 2 a common primitive root of p and q, so that 2 is a strong primitive λ-root of n. Write $a \equiv -2^{\lambda(n)/2}$, $b \equiv 2^{-1}(a+1)$ and $c \equiv -2^{-1}(a-1) \pmod n$, whence $q|b$ and $p|c$. Then the sequence*

$$2^1 a\ \ 2^2 a\ \ \ldots\ \ 2^{\lambda(n)-1} a\ \ a\ \mid\ 2^1 b\ \ 2^2 b\ \ \ldots\ \ 2^{p-2} b\ \ b\ \mid$$
$$0\ \mid\ c\ \ 2^{q-2} c\ \ 2^{q-3} c\ \ \ldots\ \ 2^1 c\ \mid\ 1\ \ 2^{\lambda(n)-1}\ \ 2^{\lambda(n)-2}\ \ \ldots\ \ 2$$

is a $\mathbb{Z}_n$ terrace with the units of $\mathbb{Z}_n$ in the first and last segments.

Proof. Checking that $a \equiv 1 \pmod p$ and $a \equiv -1 \pmod q$ is routine. The rest of the proof is standard. □

Note: In the range $n < 200$ with $q > 3$, Theorem 3.3 provides $\mathbb{Z}_n$ terraces for $n = 55$, 95 and 143.

Example 3.3. $(n, p, q) = (55, 5, 11)$.
We have the $\mathbb{Z}_{55}$ terrace

$$42 \;\; 29 \;\; \ldots \;\; 21 \;\; | \;\; 22 \;\; 44 \;\; 33 \;\; 11 \;\; | \;\; 0 \;\; | \;\; 45 \;\; 50 \;\; \ldots \;\; 35 \;\; | \;\; 1 \;\; 28 \;\; \ldots \;\; 2.$$

3.2. Terraces with zero in the first segment

We now use $I_{n,q}$ to denote the member of $\mathbb{Z}_n$ that is a multiple of q and is one greater than a multiple of p. The importance of this element in the construction of terraces for $\mathbb{Z}_n$ was demonstrated in [4]. The notation reflects the fact that this member of $\mathbb{Z}_n$ is the identity element of the group of multiples of q under multiplication modulo n. Also, given a primitive λ-root x of n, we define the set S_x more generally than in Section 2 to be $S_x = \{1, x, \ldots, x^{\lambda(n)-1}\}$; it contains $\lambda(n) = (p-1)(q-1)/2$ numbers.

Theorem 3.4. *Let $n = pq$ where p and q are distinct odd primes satisfying* $\gcd(p-1, q-1) = 2$ *and where 2 is a primitive root of p. Suppose that there exists a primitive λ-root x of n satisfying $2x \equiv 1 \pmod p$, $2x \not\equiv 1 \pmod q$ and $2 - x$ is a unit not in S_x. Take $a \equiv (2-x)x^{-1} \pmod n$, and take $b = a(2x-1)$, so that $p|b$. Define y by $y \equiv 1 \pm ((I_{n,q}-1)/p)(b/p)^{-1} \pmod q$. Then if y is a primitive root of q, the sequence*

$$0 \;\; | \;\; 2^{p-2}I_{n,q} \;\; 2^{p-3}I_{n,q} \;\; \ldots \;\; I_{n,q} \;\; | \;\; 1 \;\; x \;\; \ldots \;\; x^{\lambda(n)-1} \;\; |$$

$$a \;\; ax^{\lambda(n)-1} \;\; ax^{\lambda(n)-2} \;\; \ldots \;\; ax \;\; | \;\; b \;\; by^{q-2} \;\; by^{q-3} \;\; \ldots \;\; by$$

is a $\mathbb{Z}_n$ terrace with the units of $\mathbb{Z}_n$ in the third and fourth segments.

Proof. Both of the relationships $f_1 = -m_1 = -2^{-1}I_{n,q}$ and $f_2 = \pm m_4$ are immediate. Also $f_3 = a - x^{-1} = (2 - x - 1)x^{-1} = (1-x)x^{-1} = -m_2$ and $f_4 = b - ax = a(x-1) = -m_3$. □

Note (a): If $x = 3$ (a strong primitive λ-root of n) and $a = -3^{-1}$, then $b = 3^{-1} - 2$. The fourth segment of the terrace is then the negative of the reverse of the third.

Note (b): Parameter sets for $\mathbb{Z}_n$ terraces available from Theorem 3.4 are as follows, where $^{\text{neg}}$ again indicates a negating primitive λ-root, the other primitive λ-roots in the table all being strong:

n	p	q	$I_{n,q}$	x	a	y	b	Note
35	5	7	21	3	23	3	10	(a)
55	5	11	11	3	18	6 or 7	35	(a)
	11	5	45	—	—	—	—	
77	11	7	56	61^{neg}	47	3	66	
95	5	19	76	3	63	13	30	(a)
	19	5	20	—	—	—	—	
115	5	23	46	3	38	5 or 20	75	(a)
143	11	13	78	—	—	—	—	
	13	11	66	85	68	8	52	
155	5	31	31	43	118	12 or 21	110	
187	11	17	34	6	124	5 or 14	55	

Example 3.4. $(n, p, q) = (35, 5, 7)$.

Use $(x, a, y, b) = (3, 23, 3, 10)$ to give the $\mathbb{Z}_{35}$ terrace

$$0 \mid 28 \; 14 \; 7 \; 21 \mid 1 \; 3 \; \ldots \; 12 \mid 23 \; 31 \; \ldots \; 34 \mid 10 \; 15 \; \ldots \; 30.$$

Theorem 3.5. *Let $n = pq$ where p and q are distinct odd primes such that $\gcd(p-1, q-1) = 2$ and such that 2 is a primitive root of p. Let x be a primitive λ-root of n, with $x \equiv 2 \pmod p$, $x \not\equiv 2 \pmod n$. Define $b = (2-x)x^{-1}$, so that $p|b$. Define y by $y \equiv 1 \pm x(2-x)^{-1} \pmod q$. Then if y is a primitive root of q, there exists a unit a such that*

$$0 \mid 2^{p-2}I_{n,q} \; 2^{p-3}I_{n,q} \; \ldots \; I_{n,q} \mid 1 \; x \; \ldots \; x^{\lambda(n)-1} \mid$$

$$b \; by^{q-2} \; by^{q-3} \; \ldots \; by \mid a \; ax^{\lambda(n)-1} \; ax^{\lambda(n)-2} \; \ldots \; ax$$

is a $\mathbb{Z}_n$ terrace with the units of $\mathbb{Z}_n$ in the third and fifth segments.

Proof. Define $\alpha \equiv yx^{-1} \pmod q$. Then, for all μ, the values $a_\mu = \alpha + \mu q$ are solutions of the congruence $by \equiv a_\mu(2-x) \pmod n$. Precisely, one of these values a_μ, $0 \leqslant \mu \leqslant p-1$, will be a multiple of p, so $p-1$ of the values will be units.

If x is a primitive root of q, then, modulo q, the set S_x contains a complete set of residues exactly $(p-1)/2$ times. So, in particular, S_x contains $(p-1)/2$ numbers that are congruent to α, modulo q, i.e. S_x contains exactly $(p-1)/2$ of the numbers α_μ. Thus there are $(p-1)/2$ units α_μ that are not in S_x. Take any one of these as a.

If $\mathrm{ord}_q(x) = (q-1)/2$, then, modulo q, the set S_x contains $(q-1)/2$ members of a complete set of residues, each $p-1$ times. So either none or all of the values a_u will be in S_x. But in fact *none* of the values a_u is in S_x. For if $a_u \in S_x$ then $yx^{-1} \equiv x^i \pmod q$ for some i, so that y is a power of $x \pmod q$. But x is not a primitive root of q, and hence y

cannot be a primitive root of q, which gives us a contradiction. So, as none of the values a_u is in S_x, we can take a to be any one of them except for the one that is a multiple of p.

For a $\mathbb{Z}_n$ terrace, we need $I_{n,q} - 1 = \pm b(y-1)$, $by = a(2-x)$ and $b = (2-x)x^{-1}$. The first of these requires $b(y-1) \equiv \pm 1 \pmod q$, i.e. $y - 1 \equiv \pm x(2-x)^{-1} \pmod q$, i.e. $y \equiv 1 \pm x(2-x)^{-1} \pmod q$. The second requires $y \equiv ax \pmod q$. $\square$

Note (a): Terraces of the form given in Theorem 3.5 are obtainable from the following parameter sets, in each of which the primitive λ-root x is a common primitive root of p and q; again the only negating primitive λ-root in the table is for $n = 77$:

n	p	q	$I_{n,q}$	x	a	y	b
35	5	7	21	12	$8x^{6i}$, $0 \leqslant i \leqslant 1$	5	5
55	5	11	11	52	$42x^{10i}$, $0 \leqslant i \leqslant 1$	6	35
	11	5	45	13	$6x^{4i}$, $0 \leqslant i \leqslant 4$	3	33
77	11	7	56	24^{neg}	$18x^{6i}$, $0 \leqslant i \leqslant 4$	5	44
95	5	19	76	72	$68x^{18i}$, $0 \leqslant i \leqslant 1$	13	65
	19	5	20	78	$21x^{4i}$, $0 \leqslant i \leqslant 8$	3	38
115	5	23	46	107	$13x^{22i}$, $0 \leqslant i \leqslant 1$	11	85
143	11	13	78	24	$29x^{12i}$, $0 \leqslant i \leqslant 4$	7	11
	13	11	66	28	$5x^{10i}$, $0 \leqslant i \leqslant 5$	8	91
155	5	31	31	42	$72x^{30i}$, $0 \leqslant i \leqslant 1$	17	95
187	11	17	34	24	$32x^{16i}$, $0 \leqslant i \leqslant 4$	3	77

Note (b): Terraces of the form given in Theorem 3.5 are obtainable also from the following parameter sets, where the primitive λ-root x of n is a primitive root of p but $\mathrm{ord}_q(x) = (q-1)/2$; now the primitive λ-root used for $n = 77$ is strong:

n	p	q	$I_{n,q}$	x	a	y	b
77	11	7	56	46	$6x^{3i}$, $0 \leqslant i \leqslant 9$	3	66
95	5	19	76	42	$11x^{9i}$, $0 \leqslant i \leqslant 3$	3	85
115	5	23	46	52	$33x^{11i}$, $0 \leqslant i \leqslant 3$	14	30
143	13	11	66	119	$8x^{5i}$, $0 \leqslant i \leqslant 11$	6	130
155	5	31	31	7	$3x^{15i}$, $0 \leqslant i \leqslant 3$	21	110

Example 3.5. $(n, p, q) = (35, 5, 7)$.

The congruences $x \equiv 2 \pmod 5$ and $x \equiv 3$ or $5 \pmod 7$ yield the two possibilities $x = 12$ and 17. The former allows us to use $(x, a, y, b) = (12, 8, 5, 5)$ to obtain the $\mathbb{Z}_{35}$ terrace

$$0 \mid 28\ 14\ 7\ 21 \mid 1\ 12\ \ldots\ 3 \mid 5\ 15\ \ldots\ 25 \mid 8\ 24\ \ldots\ 26.$$

3.3. Terraces with zero in the second segment

Theorem 3.6 (*Generalisation of Theorem 2.8*). *Let $n = pq$ where p and q are odd primes, $q > 3$, such that $\gcd(p-1, q-1) = 2$ and where 2 is a common primitive root of p and q. Let x be a primitive λ-root of n that satisfies $2x \equiv 1 \pmod p$. Then $1 - x$ is a unit of $\mathbb{Z}_n$. Write $a = (1-x)^{-1}$ and $b = (1-x)^{-1} - x^{-1}$. Then $a \equiv 2 \pmod p$ and $p|b$. If $a \notin S_x$, the sequence*

$$2^0q \quad 2^1q \quad \ldots \quad 2^{p-2}q \quad | \quad 0 \quad | \quad 1 \quad x \quad x^2 \quad \ldots \quad x^{\lambda(n)-1} \quad |$$
$$a \quad ax^{\lambda(n)-1} \quad ax^{\lambda(n)-2} \quad \ldots \quad ax \quad | \quad b \quad 2^{q-2}b \quad 2^{q-3}b \quad \ldots \quad 2b$$

is a $\mathbb{Z}_n$ terrace with the units of $\mathbb{Z}_n$ in the third and fourth segments.

Proof. Straightforward. □

Note (a): In any terrace obtainable from this or the next theorem, the first segment may of course be multiplied throughout by any power of 2.

Note (b): A special case of Theorem 3.6 has $x = x^2 - 1 = x^{-1} + 1$ and $a = ax^{\lambda(n)-2} - 1 = ax + 1 = -x$, whence $b = 1 - 2x$ where x is non-negating. For $n = 55$ and 95 (see table below), primitive λ-roots x satisfying these relationships occur in pairs x_1 and x_2 with $x_1x_2 \equiv -1 \pmod n$ and $x_1 \equiv x_2 \pmod 5$; the final segment of the $\mathbb{Z}_n$ terrace using $p = 5$ and primitive λ-root x_1 is the negative of the final segment of the corresponding $\mathbb{Z}_n$ terrace using x_2, as $x_1 + x_2 \equiv 1 \pmod n$.

Note (c): In the range $n < 200$, Theorem 3.6 with $p, q > 3$ covers the values $n = 55$, 95 and 143, with parameter sets as follows:

n	p	q	(x, a, b)	
			$x^2 = x + 1$	$x^2 \neq x + 1$
55	5	11	(8, 47, 40), (48, 7, 15)	(18, 42, 45), (38, 52, 10)
	11	5	—	(17, 24, 11)
95	5	19	(43, 52, 10), (53, 42, 85)	(3, 47, 15), (13, 87, 65), (33, 92, 20), (63, 72, 75), (93, 32, 80)
	19	5	—	(67, 59, 76)
143	11	13	—	(28, 90, 44), (50, 35, 55)
	13	11	—	(7, 119, 78), (59, 106, 26), (85, 80, 117), (137, 41, 65)

Example 3.6. $(n, p, q) = (55, 5, 11)$.

Use $(x, a, b) = (18, 42, 45)$ to give the $\mathbb{Z}_{55}$ terrace

$$11 \quad 22 \quad 44 \quad 33 \quad | \quad 0 \quad | \quad 1 \quad 18 \quad \ldots \quad 52 \quad | \quad 42 \quad 39 \quad \ldots \quad 41 \quad | \quad 45 \quad 50 \quad \ldots \quad 35.$$

Theorem 3.7. *Let $n = pq$ where p and q are distinct odd primes such that* $\gcd(p-1, q-1) = 2$, *and where* 2 *is both a primitive root of p and a primitive λ-root of n. Then there exist $\phi(q-1)-1$ primitive λ-roots x of n satisfying $x \in S_2$, $2x \equiv 1 \pmod p$ and $2x \not\equiv 1 \pmod q$. For such an x, choose a unit a, not in S_2, that satisfies $a \equiv 2 \pmod p$, and take $b = a(2x-1)$, so that $p|b$. Define y by $y \equiv 1 \pm ((a-2)/p)(b/p)^{-1} \pmod q$. Then, if y is a primitive root of q, the sequence*

$$2^0q \quad 2^1q \quad \ldots \quad 2^{p-2}q \quad | \quad 0 \quad | \quad 1 \quad 2^{\lambda(n)-1} \quad 2^{\lambda(n)-2} \quad \ldots \quad 2 \quad |$$

$$a \quad ax^{\lambda(n)-1} \quad ax^{\lambda(n)-2} \quad \ldots \quad ax \quad | \quad b \quad by^{q-2} \quad by^{q-3} \quad \ldots \quad by$$

is a $\mathbb{Z}_n$ terrace with the units of $\mathbb{Z}_n$ in the third and fourth segments.

Proof. Modulo p, the set S_2 consists of exactly $(q-1)/2$ copies of the set $\{1, 2, \ldots, 2^{p-2}\}$ of units of $\mathbb{Z}_p$. So those values x from S_2 that satisfy $2x \equiv 1 \pmod p$ are precisely the values $x = 2^{k(p-1)-1}$, $1 \leqslant k \leqslant (q-1)/2$. Further, such a value x is a primitive λ-root of n precisely when we have $\gcd(k(p-1)-1, \lambda(n)) = 1$, i.e. $\gcd(k(p-1)-1, (p-1)(q-1)/2) = 1$. First suppose that $q \equiv 3 \pmod 4$. Then this condition becomes

$$\gcd(k(p-1)-1, (q-1)/2) = 1. \tag{6}$$

Now the numbers $k(p-1)-1$ are all incongruent modulo $(q-1)/2$; so exactly $\phi((q-1)/2)$ of the values of k satisfy (6). One of these values is $(q-1)/2$, which gives $2x \equiv 1 \pmod q$; so there remain $\phi((q-1)/2) - 1 = \phi(q-1) - 1$ possible choices of k and hence there are $\phi(q-1)-1$ primitive λ-roots x with the required properties.

The other possibility is $q \equiv 5 \pmod 8$. Then (6) must be replaced by

$$\gcd(k(p-1)-1, (q-1)/4) = 1. \tag{7}$$

Now the numbers $k(p-1)-1$, $1 \leqslant k \leqslant (q-1)/4$, are all incongruent modulo $(q-1)/4$, as are those given by $(q-1)/4 < k \leqslant (q-1)/2$. So there are $2\phi((q-1)/4)$ values of k satisfying (7). As before, this leads to $2\phi((q-1)/4) - 1 = \phi(q-1) - 1$ primitive λ-roots x with the required properties.

Clearly, $m_1 = -f_1$, $m_2 = -f_2$, $m_3 = -f_4$ and $m_4 = \pm f_3$. $\square$

Note (a): The set S_2 contains $(q-1)/2$ numbers that are congruent to 2 modulo p. Thus, for given x, there are $(q-1)/2$ members of $\mathbb{Z}_n$ that are congruent to $2 \pmod p$ and not in S_2. As precisely one of these is divisible by q, there are $((q-1)/2) - 1$ possible choices of a.

Note (b): If 2 is a primitive root of q, a special case of Theorem 3.7 is obtained by taking $y = 2$. Then $b = a - 2$ and so $a = (1-x)^{-1}$; we thus obtain a $\mathbb{Z}_n$ terrace provided that $(1-x)^{-1} \notin S_2$.

Note (c): As 2 is not a primitive λ-root of 155 or 187, Theorem 3.7, unlike the two preceding theorems, does not cover $n = 155$ or 187.

Note (d): Parameter sets for $\mathbb{Z}_n$ terraces obtainable from Theorem 3.7 are as follows, where all the primitive λ-roots x are strong; each line of the table gives the solution for $y = 2$, if there is one, and a specimen solution for $y \neq 2$:

n	p	q	$\phi(q-1)$	$I_{n,q}$	x	(a, y, b)	
						$y = 2$	$y \neq 2$
35	5	7	2	21	23	—	(17, 5, 30)
55	5	11	4	11	8	(47, 2, 45)	(42, 7, 25)
					13	—	(47, 6, 20)
					18	(42, 2, 40)	(12, 6, 35)
	11	5	2	45	17	(24, 2, 22)	(46, 3, 33)
77	11	7	2	56	72	—	(68, 5, 22)
95	5	19	6	76	3	(47, 2, 45)	(87, 15, 55)
					13	(87, 2, 85)	(47, 13, 35)
					33	(92, 2, 90)	(7, 15, 75)
					53	(42, 2, 40)	(87, 13, 15)
					78	—	(7, 13, 40)
	19	5	2	20	67	(59, 2, 57)	(21, 3, 38)
115	5	23	10	46	3	—	(7, 14, 35)
					8	—	(22, 15, 100)
					13	—	(17, 17, 80)
					18	—	(17, 19, 20)
					48	—	(107, 14, 45)
					73	—	(7, 7, 95)
					78	—	(7, 17, 50)
					98	—	(17, 19, 95)
					108	—	(17, 20, 90)
143	11	13	4	78	6	—	(79, 7, 11)
					28	(90, 2, 88)	(35, 7, 66)
					50	(35, 2, 33)	(68, 7, 11)
	13	11	4	66	7	(119, 2, 117)	(67, 6, 13)
					46	—	(67, 8, 91)
					85	(80, 2, 78)	(93, 8, 130)

Example 3.7. $(n, p, q) = (35, 5, 7)$.

Use $(x, a, y, b) = (23, 12, 5, 15)$ to give the $\mathbb{Z}_{35}$ terrace

$$7\ 14\ 28\ 21\ \mid\ 0\ \mid\ 1\ 18\ \ldots\ 2\ \mid\ 12\ 34\ \ldots\ 31\ \mid\ 15\ 10\ \ldots\ 5.$$

4. Terraces for $\mathbb{Z}_{pq}$ with $\xi(pq) = 4$

4.1. Terraces with zero in the fourth (middle) segment

Now, and in Sections 4.2 and 4.3, we use the following Result, which is a slight rewording of Theorems 8.5 and 8.6 of [6].

Cameron/Preece Result: Let $n = pq$ where p and q are distinct primes with $\gcd(p-1, q-1) = 4$, whence $\lambda(n) = (p-1)(q-1)/4$. Let p and q also satisfy either

(a) $p \equiv q \equiv 5 \pmod 8$ and 2 is a common primitive root of p and q, or
(b) $p \equiv 1 \pmod{16}$, $q \equiv 5 \pmod 8$, $\mathrm{ord}_q(2) = q-1$ and $\mathrm{ord}_p(2) = (p-1)/2$.

Then there exists a strong primitive λ-root x of n such that $(x-1)^2 \equiv -1 \pmod n$, and the set of units of $\mathbb{Z}_n$ can be written as $S_x \cup -S_x \cup aS_x \cup -aS_x$ where $a = 1 - x$ and $S_x = \{1, x, x^2, \ldots, x^{\lambda(n)-1}\}$. Further, if $q = 5$, there exist two such values of x, respectively, with $x \equiv 3$ and $x \equiv 4 \pmod 5$.

Theorem 4.1. *Let $n = pq$ where p and q are distinct primes, both congruent to* $5 \pmod 8$, *satisfying the conditions of the Cameron/Preece Result. With x and a as in the Result, choose α and β so that $2^\alpha p \equiv -ax \pmod q$ and $2^\beta q \equiv ax \pmod p$. Then*

$$2^{\alpha+1}p \;\; 2^{\alpha+2}p \;\; \ldots \;\; 2^{\alpha-1}p \;\; 2^\alpha p \;\; | \;\; -ax \;\; -ax^2 \;\; \ldots \;\; -ax^{\lambda(n)-1} \;\; -a \;\; |$$

$$-x^{\lambda(n)-1} \;\; -x^{\lambda(n)-2} \;\; \ldots \;\; -x \;\; -1 \;\; | \;\; 0 \;\; | \;\; 1 \;\; x \;\; \ldots \;\; x^{\lambda(n)-2} \;\; x^{\lambda(n)-1} \;\; |$$

$$a \;\; ax^{\lambda(n)-1} \;\; \ldots \;\; ax^2 \;\; ax \;\; | \;\; 2^\beta q \;\; 2^{\beta-1}q \;\; \ldots \;\; 2^{\beta+2}q \;\; 2^{\beta+1}q$$

is a $\mathbb{Z}_n$ terrace where the units of $\mathbb{Z}_n$ are in the second, third, fifth and sixth segments.

Proof. We have $m_1 = 2^\alpha p$, $m_2 = m_5 = a(1-x)$, $m_3 = m_4 = x^{\lambda(n)-1}(x-1)$ and $m_6 = -2^\beta q$. Also $f_1 = -2^\alpha p - ax$, $f_2 = f_5 = a - x^{\lambda(n)-1}$, $f_3 = f_4 = 1$ and $f_6 = 2^\beta q - ax$. Thus $m_2 = -f_3$ and $m_5 = f_4$; also $f_5 = f_2 = a - x^{\lambda(n)-1} = a - x^{-1} = (ax-1)x^{-1} = (1-x)x^{-1} = -m_3 = -m_4$. Modulo p we have $m_1 \equiv 0 \equiv f_6$, and modulo q we have $m_1 \equiv 2^\alpha p \equiv -ax \equiv f_6$; so $m_1 \equiv f_6 \pmod n$. Similarly, $m_6 \equiv f_1 \pmod n$. $\square$

Note (a): The symmetry of the construction embodied in Theorem 4.1 is such that, once a solution has been found, an alternative can be obtained by merely interchanging p and q, replacing β by the original $\alpha + (q-1)/2 \pmod{q-1}$, and replacing the original α by the original $\beta + (p-1)/2 \pmod{p-1}$.

Note (b): In the range $n < 200$ Theorem 4.1 covers $n = 65$, 145 and 185. For each of these values of n there are, as the Cameron/Preece Result indicates, two primitive λ-roots x_1 and x_2, satisfying $x_1 \equiv 3 \pmod 5$ and $x_2 \equiv 4 \pmod 5$, each of which meets the conditions imposed on the primitive λ-root x. These primitive λ-roots further satisfy $x_1 + x_2 \equiv x_1x_2 \equiv 2 \pmod n$ and therefore $x_1^2 \equiv -x_2^2 \pmod n$, Sets of parameter values for the $\mathbb{Z}_n$ terraces obtainable are as follows:

n	x	a	(p, q, α, β)
65	48	18	(13, 5, 1, 8) or (5, 13, 2, 3)
	19	47	(13, 5, 2, 11) or (5, 13, 5, 4)
145	13	133	(29, 5, 2, 17) or (5, 29, 3, 0)
	134	12	(29, 5, 3, 24) or (5, 29, 10, 1)
185	118	68	(37, 5, 3, 18) or (5, 37, 0, 1)
	69	117	(37, 5, 0, 9) or (5, 37, 27, 2)

Example 4.1. $(n, p, q) = (65, 5, 13)$.

Use $(x, a, \alpha, \beta) = (48, 18, 2, 3)$ to obtain the $\mathbb{Z}_{65}$ terrace

$$40\ \ 15\ \ \ldots\ \ 20\ \mid\ 46\ \ 63\ \ \ldots\ \ 47\ \mid\ 23\ \ 56\ \ \ldots\ \ 64\ \mid\ 0\ \mid$$
$$1\ \ 48\ \ \ldots\ \ 42\ \mid\ 18\ \ 41\ \ \ldots\ \ 19\ \mid\ 39\ \ 52\ \ 26\ \ 13.$$

Theorem 4.2. *Let $n = 5p$ where p is a prime, $p \equiv 1 \pmod 4$, $p > 5$, having 2×3^{-1} as a primitive root. Choose x from the units of $\mathbb{Z}_n$ so that $x \equiv 2 \times 3^{-1} \pmod p$ and $x \equiv 4 \pmod 5$. Then x is a strong primitive λ-root of n. Choose α, β and γ so that $x^\gamma \equiv \pm x(x-1)^{-1} \pmod p$, $x^\alpha \equiv -3 \times 5^{-1} x^\gamma \pmod p$ and $3^{\beta-1} p \equiv 1 \pmod 5$. Then*

$$5x^{\alpha-1}\ \ 5x^{\alpha-2}\ \ \ldots\ \ 5x^{\alpha}\ \mid\ -2x^{\gamma-1}\ \ -2x^{\gamma-2}\ \ \ldots\ \ -2x^{\gamma}\ \mid$$
$$-x^{\gamma-1}\ \ -x^{\gamma-2}\ \ \ldots\ \ -x^{\gamma}\ \mid\ 0\ \mid\ x^0\ \ x^1\ \ \ldots\ \ x^{\lambda(n)-1}\ \mid$$
$$2x^0\ \ 2x^1\ \ \ldots\ \ 2x^{\lambda(n)-1}\ \mid\ 3^{\beta}p\ \ 3^{\beta+1}p\ \ \ldots\ \ 3^{\beta-1}p$$

is a $\mathbb{Z}_n$ terrace where the units of $\mathbb{Z}_n$ are in the second, third, fifth and sixth segments.

Proof. As $\mathrm{ord}_n(x) = \mathrm{lcm}(2, p-1) = p-1$, the unit x is a primitive λ-root of n. It is non-negating as, if $x^i \equiv -1 \pmod n$, then $x^i \equiv 4 \pmod 5$, so that i is odd, and $x^i \equiv -1 \pmod p$, so that i is even. It is inward as $x - 1 \not\equiv 0 \pmod 5$ and $x - 1 \not\equiv 0 \pmod p$. Further, neither 2 nor -2 is a power of x; for if $x^j \equiv \pm 2 \pmod n$ then $4^j \equiv \pm 2 \pmod 5$, an impossibility.

As $x \equiv 2 \times 3^{-1} \pmod n$, the relationships $m_2 = -f_3$, $m_3 = -f_2$, $m_4 = -f_5$ and $m_5 = -f_4$ are easily checked.

We now show that $m_1 = \pm f_6$ and $m_6 = \pm f_1$. Modulo 5 we have $m_1 = 5x^{\alpha-1}(x-1)$ and $f_6 = 3^\beta p - 3$, whence $f_6 = 3(3^{\beta-1}p - 1) \equiv 0 \equiv \pm m_1$, whereas modulo p we have $m_1 \equiv (x-1)x^{-1} \times 3x^\gamma \equiv \pm 3 \equiv \pm f_6$.

Finally, we show that $m_6 = \pm f_1$, where $m_6 = 2p \times 3^{\beta-1}$ and $f_1 = -2x^{\gamma-1} - 5x^\alpha$. So modulo 5 we have $f_1 \equiv -2x^{\gamma-1} \equiv -2 \times 4^{\gamma-1} \equiv \pm 2 \equiv \pm m_6$, whereas modulo p we have $f_1 \equiv -2x^{\gamma-1} + 3x^\gamma \equiv (3x-2)x^{\gamma-1} \equiv 0 \equiv \pm m_6$. $\square$

Note: For each value of n, Theorem 4.2 yields two $\mathbb{Z}_n$ terraces, given by values of γ that differ by $(p-1)/2$. Changing from one value to the other causes the first segment to be replaced by its negative, but the second and third segments change to a greater extent, with α also changing by $(p-1)/2$. For the range $n < 200$, sets of parameter values for the terraces obtained are as follows:

n	p	x	α	β	γ
85	17	29	2	2	14
			10	2	6
185	37	124	20	2	5
			2	2	23

Example 4.2. $(n, p) = (85, 17)$.

The parameters $(x, \alpha, \beta, \gamma) = (29, 2, 2, 14)$ give the $\mathbb{Z}_{85}$ terrace

$$60 \;\; 90 \;\; \ldots \;\; 40 \;\mid\; 57 \;\; 43 \;\; \ldots \;\; 38 \;\mid\; 71 \;\; 64 \;\; \ldots \;\; 19 \;\mid\; 0 \;\mid$$

$$1 \;\; 29 \;\; \ldots \;\; 44 \;\mid\; 2 \;\; 58 \;\; \ldots \;\; 3 \;\mid\; 68 \;\; 34 \;\; 17 \;\; 51.$$

4.2. Terraces with zero in the first segment

With $n = 5p$, we now use $I_{n,p}$ to denote the member of $\mathbb{Z}_n$ that is a multiple of p and is one greater than a multiple of 5.

Theorem 4.3. *Let $n = 5p$ where p is a prime, $p > 5$, satisfying the conditions of the Cameron/Preece Result with $q = 5$. Taking x and a as in the Result, with $x \equiv 4 \pmod 5$, define $c = 3 - 2x$, so that $5|c$. Define y by $c(y-1) \equiv \pm(I_{n,p} - 1)$. Then, if y is a primitive root of p, the arrangement*

$$0 \;\mid\; 2^3 I_{n,p} \;\; 2^2 I_{n,p} \;\; 2^1 I_{n,p} \;\; 2^0 I_{n,p} \;\mid$$

$$x^0 \;\; x^{p-2} \;\; x^{p-3} \;\; \ldots \;\; x \;\mid\; -ax^0 \;\; -ax^{p-2} \;\; -ax^{p-3} \;\; \ldots -ax \;\mid$$

$$-x^0 \;\; -x^{p-2} \;\; -x^{p-3} \;\; \ldots \;\; -x \;\mid\; ax^0 \;\; ax^{p-2} \;\; ax^{p-3} \;\; \ldots \;\; ax \;\mid$$

$$c \;\; cy^{p-2} \;\; cy^{p-3} \;\; \ldots \;\; cy$$

is a $\mathbb{Z}_n$ terrace with the units of $\mathbb{Z}_n$ in the third to sixth segments inclusive.

Proof. The following relationships are easily checked: $m_1 = -f_1$, $m_2 = f_6$, $m_3 = -f_3$, $m_4 = f_4$, $m_5 = -f_5$ and $m_6 = \pm f_2$. $\square$

Note: In the range $n < 200$, Theorem 4.3 yields $\mathbb{Z}_n$ terraces for $n = 65$, 85 and 145. (It fails for $n = 185$ as no primitive root y is available.) Parameter sets are as follows:

n	p	$I_{n,p}$	x	a	c	y
65	13	26	19	47	30	11
85	17	51	14	72	60	3
145	29	116	134	12	25	8

Example 4.3. $(n, p) = (65, 13)$.

With $(I_{n,p}, x, a, c, y) = (26, 19, 47, 30, 11)$, Theorem 4.3 produces the $\mathbb{Z}_{65}$ terrace

$$0 \mid 13\ \ 39\ \ 52\ \ 26 \mid 1\ \ 24\ \ \ldots\ \ 19 \mid 18\ \ 42\ \ \ldots\ \ 17 \mid$$
$$64\ \ 41\ \ \ldots\ \ 46 \mid 47\ \ 23\ \ \ldots\ \ 48 \mid 30\ \ 50\ \ \ldots\ \ 5.$$

4.3. Terraces with zero in the second segment

Theorem 4.4. *Let $n = 5p$ where p is a prime, $p > 5$, satisfying the conditions of the Cameron/Preece Result with $q = 5$. Taking x and a as in the Result, with $x \equiv 3 \pmod 5$, choose b from $-S_x$ such that $b \equiv 4 \pmod 5$, and define $c = ab(2x-1) = b(3-x)$, so that $5|c$. Define w by $c(w-1) = \pm(b-ax)$. Then, if w is a primitive root of p, the arrangement*

$$2^0p\ \ 2^1p\ \ 2^2p\ \ 2^3p \mid 0 \mid$$
$$x^0\ \ x^1\ \ \ldots\ \ x^{p-2} \mid a\ \ ax^{p-2}\ \ ax^{p-3}\ \ \ldots\ \ ax \mid$$
$$bx^0\ \ bx^1\ \ \ldots\ \ bx^{p-2} \mid ab\ \ abx^{p-2}\ \ abx^{p-3}\ \ \ldots\ \ abx \mid$$
$$c\ \ cw^{p-2}\ \ cw^{p-3}\ \ \ldots\ \ cw$$

is a $\mathbb{Z}_n$ terrace with the units of $\mathbb{Z}_n$ in the third to sixth segments inclusive.

Proof. We have $m_1 = -f_1$, $m_2 = -f_3$, $m_3 = -f_2$, $m_4 = -f_5$, $m_5 = -f_6$ and $m_6 = \pm f_4$. □

Note (a): In any terrace obtained from this theorem, the first segment may of course be multiplied throughout by any power of 2.

Note (b): If $b = -1$ is a valid choice, then $c = x - 3$ and $w = 2$. So no solution with $b = -1$ exists if $p \equiv 1 \pmod{16}$ as 2 is then a square. For $p \equiv 5 \pmod 8$ however, a solution always exists with $b = -1$ and $w = 2$.

Note (c): In $-S_x$ there are $(p-1)/4$ units congruent to $4 \pmod 5$, namely $-x^0, -x^4, -x^8, \ldots, -x^{p-5}$. Whether any particular such value can be chosen for b depends entirely on whether the corresponding value w is a primitive root of p. As stated in Note (b) above, there is always at least one solution if $p \equiv 5 \pmod 8$.

Note (d): Parameter sets for $\mathbb{Z}_n$ terraces obtainable from Theorem 4.4 include the following:

n	p	x	a	b	c	w
65	13	48	18	$64 = -x^0$	45	2
				$4 = -x^4$	15	2
				$49 = -x^8$	5	7
85	17	48	38	$4 = -x^4$	75	6
				$69 = -x^8$	40	6
				$64 = -x^{12}$	10	12
		73	13	$69 = -x^8$	15	3
				$64 = -x^{12}$	25	3
145	29	13	133	$144 = -x^0$	10	2
				$4 = -x^4$	105	26
				$129 = -x^8$	15	8
				$34 = -x^{16}$	95	3
				$9 = -x^{20}$	35	14
				$109 = -x^{24}$	70	11
185	37	118	68	$184 = -x^0$	115	2
				$64 = -x^{12}$	40	24
				$99 = -x^{20}$	85	5
				$159 = -x^{24}$	30	35
				$139 = -x^{32}$	110	5

Example 4.4. $(n, p) = (85, 17)$.
Use $(x, a, b, c, w) = (73, 13, 69, 15, 3)$ to give the $\mathbb{Z}_{85}$ terrace

$$17\ \ 34\ \ 68\ \ 51\ \mid\ 0\ \mid\ 1\ \ 73\ \ \ldots\ \ 7\ \mid\ 13\ \ 6\ \ \ldots\ \ 14\ \mid$$
$$69\ \ 22\ \ \ldots\ \ 58\ \mid\ 47\ \ 74\ \ \ldots\ \ 31\ \mid\ 15\ \ 5\ \ \ldots\ \ 45.$$

Theorem 4.5. *Let $n = 5p$ where p is a prime satisfying $p \equiv 5 \pmod 8$ and having 2 as a primitive root. Let x be a primitive λ-root of n with $x \equiv 4 \pmod 5$. Suppose that the element a, defined by $a \equiv 2x^{-1} - 1 \pmod n$, is a unit satisfying $a \notin S_x$, and that b, defined by $b = a(2x - 1)$, is a unit satisfying $b \notin S_x \cup aS_x$. Write $c \equiv 1 - ab(1 - x) \pmod n$, so that $5|c$. Then*

$$2^0p\ \ 2^1p\ \ 2^2p\ \ 2^3p\ \mid\ 0\ \mid\ 2^{p-2}c\ \ 2^{p-3}c \ldots\ \ 2^0c\ \mid$$
$$x^0\ \ x^1\ \ \ldots\ \ x^{p-2}\ \mid\ a\ \ ax^{p-2}\ \ ax^{p-3}\ \ \ldots\ \ ax\ \mid$$
$$bx^0\ \ bx^1\ \ \ldots\ \ bx^{p-2}\ \mid\ ab\ \ abx^{p-2}\ \ abx^{p-3}\ \ \ldots\ \ abx$$

is a $\mathbb{Z}_n$ terrace with the units of $\mathbb{Z}_n$ in the fourth to seventh segments inclusive.

Proof. Straightforward. □

Note: Solutions arise in pairs, the primitive λ-root in one solution being the inverse of that in another solution having the same value of b. In the range $n < 200$, solutions are as follows:

n	p	x	a	b	c
65	13	19	47	49	50
		24	37	49	35
145	29	69	102	54	10
		124	137	54	65
185	37	24	107	34	55
		54	47	34	150
		109	72	84	50
		129	32	84	150

Example 4.5. $(n, p) = (65, 13)$.

The parameters $(x, a, b, c) = (19, 47, 49, 50)$ give the $\mathbb{Z}_{65}$ terrace

$$13\ \ 26\ \ 52\ \ 39\ \ |\ \ 0\ \ |\ \ 25\ \ 45\ \ \ldots\ \ 50\ \ |\ \ 1\ \ 19\ \ \ldots\ \ 24\ \ |$$

$$47\ \ 23\ \ \ldots\ \ 48\ \ |\ \ 49\ \ 21\ \ \ldots\ \ 6\ \ |\ \ 28\ \ 22\ \ \ldots\ \ 12.$$

5. The "powers of 2 and 3" construction

5.1. Terraces with zero surrounded by units

In previous sections we have constructed $\mathbb{Z}_n$ terraces for n-values with $\xi(n) = 2$ or 4. In the range $n < 200$ there are also two n-values, namely 91 and 133, with $\xi(n) = 6$ and $n = pq$ where p and q are distinct odd primes. For each of these two n-values, power-sequence terraces with the minimum number of segments, namely 9, are easily written down via an approach which, in the range $n < 200$, can also be used for the n-values 65 and 185 (with $\xi(n) = 4$, and thus with 7 segments per terrace) and, in a degenerate form, for $n = 35$, 55 and 77 (with $\xi(n) = 2$ and thus 5 segments per terrace). This *Powers of* 2 *and* 3 approach (P2&3) can be used whenever the units of $\mathbb{Z}_n$ can all be written in the form

$$2^j \times 3^k, \quad j = 0, 1, \ldots, \lambda(n) - 1, \quad k = 0, 1, \ldots, \xi(n) - 1.$$

Thus 2 must be a primitive λ-root of n, and 3 must be a unit of order at least $\xi(n)$ such that none of the values 3^k ($k = 0, 1, \ldots, \xi(n) - 1$) is a power of 2. In the range $n < 200$, these conditions are met as follows:

n	$\lambda(n)$	$\xi(n)$	Primitive λ-root 2	Is 3 a primitive λ-root?	$3^{\xi(n)}$
35	12	2	strong	yes	2^{-2}
55	20	2	strong	yes	2^{6}
65	12	4	negating	yes	2^{4}
77	30	2	strong	yes	2^{16}
91	12	6	strong	no	1
133	18	6	strong	yes	2^{6}
185	36	4	negating	yes	2^{-4}

Outside the range $n < 200$, the conditions can of course be met when $\xi(n)$ is much larger; for example, if $n = 19 \times 37 = 703$ then $\xi(n) = 18$, the primitive λ-root 2 is strong, and $3^{\xi(n)} = 1$.

The core idea of the P2&3 approach is incorporated in Theorems 5.1 and 5.3 of [2], and in the final terrace of Section 7 from [2]. We now employ this idea in a different context, with new ramifications and new notation. We do this by first considering the following sequence $\mathscr{S}_{0,n}$ of segments for an n-value satisfying the conditions set out in the previous paragraph:

$$\begin{gathered}0 \quad | \quad 1 \quad 2^{\lambda(n)-1} \quad 2^{\lambda(n)-2} \quad \ldots \quad 2^1 \quad | \\ 2^2 \times 3^{-1} \quad 2^3 \times 3^{-1} \quad \ldots \quad 2^{\lambda(n)-1} \times 3^{-1} \quad 3^{-1} \quad 2 \times 3^{-1} \quad | \\ 2^2 \times 3^{-2} \quad 2^3 \times 3^{-2} \quad \ldots \quad 2^{\lambda(n)-1} \times 3^{-2} \quad 3^{-2} \quad 2 \times 3^{-2} \quad | \quad \ldots \quad | \\ 2^2 \times 3^{1-\xi(n)} \quad 2^3 \times 3^{1-\xi(n)} \quad \ldots \quad 2^{\lambda(n)-1} \times 3^{1-\xi(n)} \quad 3^{1-\xi(n)} \quad 2 \times 3^{1-\xi(n)}\end{gathered}$$

Here, each successive element in the *first* non-zero segment is obtained from the previous element by *dividing* by 2, but in *each other* non-zero segment each successive element is obtained by *multiplying* by 2. The important property of this sequence of segments is that $f_i = -m_i$ for $i = 1, 2, \ldots, \xi(n)$.

At this stage, a desire for simple notation suggests multiplying $\mathscr{S}_{0,n}$ throughout by 2^{-2}. However, for specific examples where algebraic notation is not needed, there is convenience in having the first non-zero segment starting with 1 and ending with 2. Then, despite the different ordering in the first non-zero segment, the final elements of the non-zero segments are easily remembered and generated as $2, 2 \times 3^{-1}, 2 \times 3^{-2}, \ldots$.

In $\mathscr{S}_{0,n}$ there are $\xi(n)$ segments *after* the zero segment, and none *before*. A more general sequence, still with $f_i = \pm m_i$ for all i, has l segments $(0 \leqslant l \leqslant \xi(n))$ after the zero, and $\xi(n) - l$ before. The rules of construction are now these:

(a) the *final* elements in the successive segments *after* the zero are $2, 2 \times 3^{-1}, \ldots, 2 \times 3^{-(l-1)}$, and the *initial* elements in the segments *before* the zero are, moving *leftwards* from the zero, $2 \times 3^{-l}, 2 \times 3^{-(l+1)}, \ldots, 2 \times 3^{-(\xi(n)-1)}$;
(b) the elements in any one segment are as in $\mathscr{S}_{0,n}$;

(c) the ordering of elements in the segments after the zero is as in $\mathscr{S}_{0,n}$ whereas that in the segments before the zero is the reverse, that is to say, each successive element in the segment *immediately* before the zero is obtained from the previous element by *multiplying* by 2, but in *each other* segment before the zero each successive element is obtained by *dividing* by 2.

We use the notation $\mathscr{S}(n, l)$ for the sequence of segments constructed in this way. Suppose, for example, that we take $l = 2$ for $n = 65$; we have

$$(2 \times 3^0,\ 2 \times 3^{-1},\ 2 \times 3^{-2},\ 2 \times 3^{-3}) = (2,\ 44,\ 58,\ 41),$$

so the sequence $\mathscr{S}(65, 2)$ is

$$41\ \ 53\ \ldots\ 17\ \mid\ 58\ \ 51\ \ldots\ 29\ \mid\ 0\ \mid\ 1\ \ 33\ \ldots\ 2\ \mid\ 23\ \ 46\ \ldots\ 44.$$

One further generalisation is needed to enable us to construct a rich collection of terraces: we multiply *all* segments to the left of the zero by 2^γ, where γ is any value satisfying $0 \leqslant \gamma < \lambda(n)$. This multiplication causes each f_i and each m_i to be multiplied by 2^γ, so the relationship between the values f_i and m_i is unchanged. We write $\mathscr{S}(n, l, \gamma)$ for the sequence after the multiplication has been done, so $\mathscr{S}(n, l, 0) = \mathscr{S}(n, l)$.

We now consider $\mathbb{Z}_n$ terraces of the form

$$cz^{p-2}\ \ cz^{p-3}\ \ \ldots\ \ c\ \mid\ \mathscr{S}(n, l, \gamma)\ \mid\ b\ \ by\ \ \ldots\ \ by^{q-2},$$

where b and c are multiples of p and q, respectively, where y and z are primitive roots of q and p, respectively, and where $0 < l < \xi(n)$. Values for b, y, c and z must be found by methodology now familiar from earlier in the paper. Examples of the $\mathbb{Z}_n$ terraces obtainable have parameter sets as follows:

n	$p<q$								$p>q$							
	p	q	l	γ	b	y	c	z	p	q	l	γ	b	y	c	z
35	5	7	1	0	30	5	14	2	7	5	1	0	7	2	10	3
55	5	11	1	0	35	7	44	2	11	5	1	1	22	3	5	7
65	5	13	1	0	15	7	26	2	13	5	1	0	52	2	15	7
			2	0	5	6	26	3			2	2	39	3	60	7
			3	1	45	11	52	3			3	0	13	2	15	6
77	7	11	1	0	35	7	66	3	11	7	1	1	44	3	49	7
91	7	13	1	0	28	6	13	5	13	7	1	2	65	5	63	7
			2	1	70	11	26	5			2	0	52	5	84	6
			3	4	84	6	26	3			3	1	78	5	77	2
			4	0	28	6	13	5			4	2	26	5	63	7
			5	1	70	11	26	5			5	0	39	5	84	6

n	$p<q$								$p>q$							
	p	q	l	γ	b	y	c	z	p	q	l	γ	b	y	c	z
133	7	19	1	0	21	14	76	5	19	7	1	2	114	5	112	10
			2	3	7	15	76	3			2	0	38	5	28	14
			3	1	91	14	19	3			3	2	57	3	112	13
			4	0	119	13	76	5			4	0	19	3	28	2
			5	0	84	15	76	3			5	3	95	5	91	13
185	5	37	1	3	150	5	148	3	37	5	1	2	37	2	125	24
			2	0	50	15	111	3			2	1	74	2	155	17
			3	0	140	20	111	2			3	0	148	2	170	18

A further related construction is available when half of the units of $\mathbb{Z}_n$ can all be written in the form

$$2^j \times 3^k, \quad j = 0, 1, \ldots, \lambda(n) - 1, \quad k = 0, 1, \ldots, (\xi(n)/2) - 1$$

but none of the remaining units can be written as a product of powers of 2 and 3. The $\mathbb{Z}_n$ terraces are now of the form

$$cz^{p-2} \;\; cz^{p-3} \;\; \ldots \;\; c \;\mid\; \mathscr{T}_{n,a} \;\mid\; b \;\; by \;\; \ldots \;\; by^{q-2},$$

where $\mathscr{T}_{n,a}$ is a sequence of $\xi(n) + 1$ segments constructed as follows, with zero in the middle segment:

(a) the successive segments *after* the zero have $2, 2 \times 3^{-1}, \ldots, 2^{1-\xi(n)/2}$ as their *final* elements;
(b) the elements in the segments after the zero, and their ordering, are as in $\mathscr{S}(n, l)$;
(c) the part of $\mathscr{T}_{n,a}$ *before* the zero is obtained by reversing the part *after* the zero and multiplying throughout by a unit a that is not already present. For $\xi(n) = 2$ this construction produces terraces that are the reverses of terraces obtainable from Theorem 3.1. In the range $n < 200$ with $\xi(n) > 2$ the construction produces $\mathbb{Z}_n$ terraces for $n = 145$ only, for which $\xi(n) = 4$; an example with $(n, p, q) = (145, 5, 29)$ has $(a, b, y, c, z) = (7, 20, 11, 58, 2)$, and an example with $(n, p, q) = (145, 29, 5)$ has $(a, b, y, c, z) = (7, 29, 2, 140, 19)$. Outside the range $n < 200$ the power of the method of construction is easily appreciated by applying it to $n = 481$, for which $\xi(n) = 12$, so that the terraces obtained have 15 segments each; an example with $(n, p, q) = (481, 13, 37)$ has $(a, b, y, c, z) = (14, 208, 17, 370, 7)$, and an example with $(n, p, q) = (481, 37, 13)$ has $(a, b, y, c, z) = (7, 370, 2, 13, 24)$.

5.2. Terraces with zero in the first segment

For values of n satisfying the conditions given at the start of the previous subsection, write $\mathscr{S}_n$ for the sequence of segments obtainable from $\mathscr{S}_{0,n}$ by removing the initial segment containing zero. We now consider $\mathbb{Z}_n$ terraces of the form

$$0 \mid 2^{p-2}I_{n,q} \;\; 2^{p-3}I_{n,q} \;\; \ldots \;\; I_{n,q} \mid \mathscr{S}_n \mid b \;\; by^{q-2} \;\; by^{q-3} \;\; \ldots \;\; by,$$

where $p|b$, with y and 2 being primitive roots of p and q respectively. The missing difference for the first segment of $\mathscr{S}_n$ is -1, and the only way of compensating for this is for the difference across the terrace's final fence to be ± 1. For $n<200$, with 2 a primitive root of p, this can be accomplished only for $(n, p, q) = (35, 5, 7)$, $(55, 5, 11)$, $(65, 5, 13)$ and $(185, 5, 37)$. However, trying $n = 185$ fails as no value of y is available with $b(1-y) \equiv \pm(1-I_{n,q})$, i.e. with $95(1-y) \equiv \pm 75 \pmod{185}$. Thus we are left with the $\mathbb{Z}_n$ terraces given by $(n, p, q, b, y) = (35, 5, 7, 25, 3)$, $(55, 5, 11, 20, 6$ or $7)$ and $(65, 5, 13, 40, 2)$. The $\mathbb{Z}_{35}$ and $\mathbb{Z}_{55}$ terraces here are of the same form as those obtainable from Theorem 3.4, but the pattern of relationships between the quantities m_i and f_i is different from that of Theorem 3.4.

5.3. Terraces with all units together at one end

For values of n satisfying the conditions given at the start of this Section and with 2 a primitive root of both p and q, we finally consider $\mathbb{Z}_n$ terraces of the form

$$\mathscr{S}_n \mid b \;\; 2b \;\; 4b \;\; \ldots \;\; 2^{q-2}b \mid 0 \mid q \;\; 2^{p-2}q \;\; 2^{p-3}q \;\; \ldots \;\; 2q,$$

where $p|b$ again. In the range $n<200$ these terraces exist only with $p=5$, and have the parameter sets given by $(n, p, q, b) = (55, 5, 11, 20)$, $(65, 5, 13, 40)$ and $(185, 5, 37, 95)$.

6. Listing of theorems and constructions

For values n that are products of two distinct odd primes and that satisfy $n<200$, Table 1 lists our theorems and constructions for $\mathbb{Z}_n$ terraces with $3+\xi(n)$ segments. The two gaps

Table 1
Theorems and constructions that provide $\mathbb{Z}_n$ terraces, $n<200$

n	Theorem or section	n	Theorem or section
15	2.1, 2.4, 2.8, 2.9	111	2.2, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9
21	2.2, 2.5, 2.6, 2.7, 2.9	115	3.1, 3.4, 3.7
33	2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9	119	—
35	3.1, 3.2, 3.4, 3.5, 3.7, §5	123	2.5, 2.6, 2.7
39	2.2, 2.4, 2.8, 2.9	129	2.7
51	2.5, 2.6, 2.7	133	§5
55	3.1, 3.3, 3.4, 3.5, 3.6, 3.7, §5	141	2.1, 2.7, 2.9
57	2.3, 2.4, 2.7, 2.8, 2.9	143	3.1, 3.3, 3.4, 3.5, 3.6, 3.7
65	4.1, 4.3, 4.4, 4.5, §5	145	4.1, 4.3, 4.4, 4.5, §5
69	2.1, 2.7, 2.9	155	3.4, 3.5
77	3.1, 3.2, 3.4, 3.5, 3.7, §5	159	2.1, 2.4, 2.7, 2.8, 2.9
85	4.2, 4.3, 4.4	161	—
87	2.1, 2.4, 2.7, 2.8, 2.9	177	2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9
91	§5	183	2.2, 2.4, 2.7, 2.8, 2.9
93	2.5, 2.6, 2.7	185	4.1, 4.2, 4.4, 4.5, §5
95	3.1, 3.3, 3.4, 3.5, 3.6, 3.7	187	3.4, 3.5

in the table are for $n = 119$ and $n = 161$, each having $\xi(n) = 2$; we have failed to find any terrace with the required properties for either of these values or indeed for any other product of two primes neither of which has 2 as a primitive root.

The concept of a terrace for a group was introduced [5] in the context of the construction of quasi-complete Latin squares. We have no reason to believe that, when the group in question is $\mathbb{Z}_n$, power-sequence terraces have any special merit for constructing other combinatorial structures. However, this paper confirms that power-sequence methodology can provide a host of simple and elegant terraces for $\mathbb{Z}_n$.

Acknowledgements

The authors are grateful to P.J. Cameron (Queen Mary, Univ. London) for very helpful discussions about primitive λ-roots and the properties of the units of $\mathbb{Z}_n$.

References

[1] I. Anderson, D.A. Preece, Locally balanced change-over designs, Util. Math. 62 (2002) 33–59.
[2] I. Anderson, D.A. Preece, Power-sequence terraces for $\mathbb{Z}_n$ where n is an odd prime power, Discrete Math. 261 (2003) 31–58.
[3] I. Anderson, D.A. Preece, Some narcissistic half-and-half power-sequence $\mathbb{Z}_n$ terraces with segments of different lengths, Congr. Numer. 163 (2003) 5–26.
[4] I. Anderson, D.A. Preece, Narcissistic half-and-half power-sequence terraces for $\mathbb{Z}_n$ with $n = pq^t$, Discrete Math. 279 (2004) 33–60.
[5] R.A. Bailey, Quasi-complete Latin squares: construction and randomisation, J. Roy. Statist. Soc. Ser. B 46 (1984) 323–334.
[6] P.J. Cameron, D.A. Preece, Notes on Primitive λ-roots, http://www.maths.qmul.ac.uk/~pjc/csgnotes/lambda.pdf
[7] R.D. Carmichael, Note on a new number theory function, Bull. Amer. Math. Soc. 16 (1909–10) 232–237.
[8] R.D. Carmichael, Generalizations of Euler's ϕ-function, with applications to Abelian groups, Quart. J. Math. 44 (1913) 94–104.
[9] R.D. Carmichael, The Theory of Numbers, Wiley, New York, 1914 (Dover, New York, 1959).
[10] S.D. Cohen, Primitive roots and powers among values of polynomials over finite fields, J. Reine Angew. Math. (Crelle's J.) 350 (1984) 137–151.