#A52 INTEGERS 12 (2012)

# OBTAINING ALL OR HALF OF $\mathbb{U}_n$ AS $\langle x\rangle \times \langle x+1\rangle$

**D. A. Preece**
*School of Mathematical Sciences, Queen Mary University of London, London, United Kingdom*
and
*School of Mathematics, Statistics and Actuarial Science, University of Kent, Canterbury, Kent, United Kingdom*
D.A.Preece@qmul.ac.uk

**Ian Anderson**
*Department of Mathematics, University of Glasgow, University Gardens, Glasgow, United Kingdom*
Ian.Anderson@glasgow.ac.uk

*Received: 11/14/11, Accepted: 7/19/12, Published: 9/21/12*

**Abstract**

For any odd positive integer $n$, let $\mathbb{U}_n$ denote the set of units of $\mathbb{Z}_n$. We investigate for which values of $n$ the set $\mathbb{U}_n$ is given by the direct product $\langle x\rangle \times \langle x+1\rangle$ for one or more values $x$, and also which are such that $\langle x\rangle \times \langle x+1\rangle$ likewise contains precisely half of the elements of $\mathbb{U}_n$. We give theorems for odd values of $n$ that are (a) prime or prime power, (b) of the form $p^iq^j$ $(i \geq 1,\ j \geq 1)$, and (c) of the form $3pq$. We provide tables giving details for all odd values of $n$ in the range $2 < n < 300$.

## 1. Introduction

### 1.1. Preliminaries

For any odd positive integer $n$, write $\mathbb{U}_n$ for the set of units of $\mathbb{Z}_n$, *i.e.* for those elements of $\mathbb{Z}_n \setminus \{0\}$ that are coprime with $n$. Thus, if $n$ is an odd prime, we have $\mathbb{U}_n = \mathbb{Z}_n \setminus \{0\}$. The number of elements in $\mathbb{U}_n$ is given by Euler's function $\phi(n) = |\,\mathbb{U}_n\,|$.

If $x \in \mathbb{U}_n$ and the value of $n$ is understood, we follow standard practice by writing $\langle x\rangle$ for the set of units of $\mathbb{Z}_n$ that are generated by $x$, *i.e.* the elements $x^0, x^1, \ldots, x^{a-1}$ where $a$ is the order of $x$ in $\mathbb{Z}_n$. We sometimes write this order as $\mathrm{ord}_n(x)$, and we use the notation $\langle x\rangle_a$ for $\langle x\rangle$ when $x$ has order $a$ in $\mathbb{Z}_n$.

In this paper, we investigate which values of $n$ have decompositions of $\mathbb{U}_n$ that are of the form $\mathbb{U}_n = \langle x \rangle \times \langle x+1 \rangle$ for one or more values $x$ from $\mathbb{U}_n$, and which values of $n$ are likewise such that $\langle x \rangle \times \langle x+1 \rangle$ contains precisely half of the elements of $\mathbb{U}_n$. (Here our use of the direct product symbol × implies that $\langle x \rangle \cap \langle x+1 \rangle = \{1\}$.) In the latter case, we often find that (a) $x(x+1) \equiv 2 \pmod{n}$, *i.e.* $(x+2)(x-1) \equiv 0 \pmod{n}$, and/or (b) no two of the $|\mathbb{U}_n|/2$ elements in $\langle x \rangle \times \langle x+1 \rangle$ are the negatives of one another, modulo $n$. Particular interest attaches to situations where conditions (a) and (b) are satisfied simultaneously.

In the range $0 < n < 300$, we find many examples where precisely half of the elements of $\mathbb{U}_n$ are obtainable from $\langle x \rangle \times \langle x+1 \rangle$ with $\langle x \rangle \times \langle x+1 \rangle = \langle 2 \rangle$.

### 1.2. Combinatorial Motivation

Study of the present topic was prompted by methodology arising in the construction of cycles of units of $\mathbb{Z}_n$ [8, 9]. For example, $\mathbb{U}_{29} = \langle 16 \rangle_7 \times \langle 17 \rangle_4$, so let us write down the multiplication table for $\langle 16 \rangle_7 \times \langle 17^{-1} \rangle_4$:

| | | | |
|---:|---:|---:|---:|
| 1 | 12 | 28 | 17 |
| 16 | 18 | 13 | 11 |
| 24 | 27 | 5 | 2 |
| 7 | 26 | 22 | 3 |
| 25 | 10 | 4 | 19 |
| 23 | 15 | 6 | 14 |
| 20 | 8 | 9 | 21 |

The successive right-minus-left differences between adjacent entries in the first row are 11, 16 and 18 (mod 29). These are the fourth, first and second entries in the second row of the table. Thus the full set of within-rows right-minus-left differences for the entire table are the entries in columns 4, 1 and 2. Likewise, the difference between the first element of row 2 and the last element of row 1 is 28, which is the third element of the first row. Thus the full set of differences between the first element in a row and the last element in the preceding row (the last row being taken to precede the first) are the entries in column 3. Accordingly, if we form a cycle by stringing together the rows of the table in their given order, with the end of the last row joined to the start of the first, we have a circular arrangement of the units of $\mathbb{Z}_{29}$ such that the differences (clockwise or anticlockwise) between adjacent elements are also precisely the units of $\mathbb{Z}_{29}$. The underlying result illustrated here is a general one for any $\mathbb{Z}_n$ ($n$ odd) that contains units $x$ and $x+1$ such that $\mathbb{U}_n = \langle x \rangle \times \langle x+1 \rangle = \langle x \rangle \times \langle (x+1)^{-1} \rangle$. Similar results are obtainable for half of the units of $\mathbb{Z}_n$, and for a third, or a quarter, *etc.*, of the units.

### 1.3. Some Examples With Small $x$

Trivially, if $n$ is a prime or prime power with 2 as a primitive root, we have $\mathbb{U}_n = \langle 1 \rangle_1 \times \langle 2 \rangle_{n-1}$. Likewise, if $n$ is a prime, prime power or composite with

$\mathrm{ord}_n(2) = \phi(n)/2$, then $\langle 1\rangle_1 \times \langle 2\rangle_{\phi(n)/2}$ gives us half of the elements of $\mathbb{U}_n$. These seemingly banal representations are important for an understanding of which values of $x$ generate all or half of $\mathbb{U}_n$ when $n$ is an odd composite. [As we see later, the reason for this is as follows: If $n$ is an odd composite and all or half of $\mathbb{U}_n$ is obtained from $\langle x\rangle \times \langle x+1\rangle$ for some $x$ with $\langle x\rangle \cap \langle x+1\rangle = \{1\}$, we find in many cases that $x$ and $x+1$ reduce, respectively, to 1 and 2 (mod $a$) where $a\,|\,n$ with $a$ and $n/a$ coprime.]

For a very few values of $n$ we have $\langle 2\rangle \times \langle 3\rangle = \mathbb{U}_n$. The smallest such prime value is $n = 683$, for which

$$\langle 2\rangle_{22} \times \langle 3\rangle_{31} = \langle n-2\rangle_{11} \times \langle n-3\rangle_{62} = \mathbb{Z}_{683} \setminus \{0\}\ .$$

The value 683 is indeed the smallest prime $n$ such that $\mathrm{ord}_n(2) = (n-1)/31$, and also the smallest such that $\mathrm{ord}_n(3) = (n-1)/22$. Amongst the first 200 000 primes, *i.e.* primes $n$ lying roughly in the range $3 < n < 2.75 \times 10^6$, the only other $n$ that has $\langle 2\rangle \times \langle 3\rangle = \mathbb{U}_n$ is 599 479, with

$$\langle 2\rangle_{33} \times \langle 3\rangle_{18\,166} = \langle n-2\rangle_{66} \times \langle n-3\rangle_{9083} = \mathbb{Z}_{599\,479} \setminus \{0\}\ .$$

Thus, for the first two primes $n$ with $\langle 2\rangle \times \langle 3\rangle = \mathbb{U}_n$, the order of 2 is a multiple of 11, and the order of 3 is a multiple of 31. For $n = 683$, clearly half of $\mathbb{U}_n$ is given by $\langle 3\rangle \times \langle 4\rangle$, whereas for $n = 599\,479$ we have $\mathbb{U}_n = \langle 3\rangle \times \langle 4\rangle$. In the quoted range there is one further prime with $\langle n-2\rangle \times \langle n-3\rangle = \mathbb{U}_n$:

$$\langle n-2\rangle_{7691} \times \langle n-3\rangle_{56} = \mathbb{Z}_{430\,697} \setminus \{0\}\ .$$

The first two non-primes with $\langle 2\rangle \times \langle 3\rangle = \mathbb{U}_n$ are $n = 91$ and 205. For these we have, respectively,

$$\langle 2\rangle_{12} \times \langle 3\rangle_6 = \mathbb{U}_{91}$$

and

$$\langle 2\rangle_{20} \times \langle 3\rangle_8 = \mathbb{U}_{205}\ .$$

Thus for $n = 91 = 7\times 13$ and $205 = 5\times 41$ the elements of $\langle 3\rangle_6 \times \langle 4\rangle_6$ and $\langle 3\rangle_8 \times \langle 4\rangle_{10}$ respectively constitute half of the set $\mathbb{U}_n$.

An intriguing situation arises when $\langle -3\rangle \times \langle -2\rangle$ gives half of $\mathbb{U}_n$ whereas $\mathbb{U}_n$ itself comes from $\langle -3\rangle \times \langle -2\rangle \times \langle -1\rangle$. This happens for the composites $n = 455 = 5\times 7\times 13$ and $n = 703 = 19 \times 37$, for which we have

$$\mathbb{U}_{455} = \langle 452\rangle_{12} \times \langle 453\rangle_{12} \times \langle 454\rangle_2$$

and

$$\mathbb{U}_{703} = \langle 700\rangle_9 \times \langle 701\rangle_{36} \times \langle 702\rangle_2\ .$$

For $n = 2593$ (prime) we have $\mathbb{U}_n = \langle 4\rangle_{81} \times \langle 5\rangle_{32}$, which is remarkable as being $\langle 4\rangle_{3^4} \times \langle 5\rangle_{2^5}$. For $n = 31$ and 601 (primes) we obtain half of $\mathbb{U}_n$ from $\langle 4\rangle_5 \times \langle 5\rangle_3$ and

$\langle 4\rangle_{25} \times \langle 5\rangle_{12}$ respectively. For $n = 93 = 3 \times 31$ we obtain half of $\mathbb{U}_n$ from $\langle 4\rangle_5 \times \langle 5\rangle_6$ , and for both $n = 217 = 7 \times 31$ and $n = 279 = 9 \times 31$ we obtain half of $\mathbb{U}_n$ from $\langle 4\rangle_{15} \times \langle 5\rangle_6$ . For $n = 63 = 3^2 \times 7$, half of $\mathbb{U}_n$ is obtained from $\langle 4\rangle_3 \times \langle 5\rangle_6$ .

For $n = 55\,987$ (prime) we have $\mathbb{U}_n = \langle 5\rangle_{7998} \times \langle 6\rangle_7$. For $n = 301 = 7 \times 43$ we have $\mathbb{U}_n = \langle 5\rangle_{42} \times \langle 6\rangle_6$, and for $n = 781 = 11 \times 71$ we obtain half of $\mathbb{U}_n$ from $\langle 5\rangle_5 \times \langle 6\rangle_{70}$.

For the prime powers $n = 25$, 37, 191 and 409, and for $n = 185 = 5 \times 37$ we have $\mathbb{U}_n = \langle 6\rangle \times \langle 7\rangle$. For $n = 311$ (prime), we obtain half of $\mathbb{U}_n$ from $\langle 6\rangle \times \langle 7\rangle$.

### 1.4. Other Examples

Not only generators, but also their orders, may differ by 1. Thus for $n = 463$ (prime) we have $\mathbb{U}_{463} = \langle 448\rangle_{22} \times \langle 449\rangle_{21}$, and for $n = 297 = 3^3 \times 11$ half of $\mathbb{U}_{297}$ is provided by $\langle 133\rangle_9 \times \langle 134\rangle_{10}$. (See also Theorem 8 below.)

Cameron and Preece [3] drew attention to classes of odd composites $n$ such that

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

for one or more units $x$. Thus for $n = 65$ we have

$$\begin{aligned} \mathbb{U}_n \quad &= \quad \langle 18\rangle_4 \times \langle 19\rangle_{12} = \langle 17\rangle_{12} \times \langle 18\rangle_4 \\ &= \quad \langle 47\rangle_4 \times \langle 48\rangle_{12} = \langle 46\rangle_{12} \times \langle 47\rangle_4 \end{aligned}$$

(see Theorem 4.1 below). Amongst primes we similarly have

$$\mathbb{U}_{569} = \langle 292\rangle_8 \times \langle 293\rangle_{71} = \langle 291\rangle_{71} \times \langle 292\rangle_8$$

for $n = 569$. Also, we now see that there are likewise primes and non-primes for which *half* of the units can be generated by

$$\langle x\rangle \times \langle x+1\rangle = \langle x-1\rangle \times \langle x\rangle$$

for one or more units $x$. Thus for $n = 131$ (prime), half of the units of $\mathbb{Z}_n$ are provided by

$$\langle 61\rangle_5 \times \langle 62\rangle_{13} = \langle 60\rangle_{13} \times \langle 61\rangle_5\ .$$

For $n = 205 = 5 \times 41$, half of the units of $\mathbb{Z}_n$ are provided by

$$\langle 132\rangle_4 \times \langle 133\rangle_{20} = \langle 131\rangle_{20} \times \langle 132\rangle_4$$

(see Theorem 4.3 below), and for $n = 259 = 7 \times 37$, half of the units of $\mathbb{Z}_n$ are provided by

$$\langle 45\rangle_{12} \times \langle 46\rangle_9 = \langle 44\rangle_9 \times \langle 45\rangle_{12}\ ;$$

in the latter example we even have $44 \equiv 46^2 \pmod{259}$.

We can also have $\mathbb{U}_n = \langle x \rangle \times \langle x+1 \rangle = \langle\, -(x-1)\, \rangle \times \langle x \rangle$. With $n = 431$ (prime), we have $\mathbb{U}_{431} = \langle 95 \rangle_5 \times \langle 96 \rangle_{43} = \langle\, -94\, \rangle_{43} \times \langle 95 \rangle_5$.

A variant of the possibility just mentioned is to obtain half of $\mathbb{U}_n$ from $\langle x \rangle \times \langle x+1 \rangle$ and all of $\mathbb{U}_n$ from $\langle x-1 \rangle \times \langle x \rangle$ with $x > 2$. This happens, for example, for the prime $n = 491$, with half of $\mathbb{U}_n$ obtainable as $\langle 381 \rangle_5 \times \langle 382 \rangle_{49}$, and with $\mathbb{U}_n = \langle 380 \rangle_{98} \times \langle 381 \rangle_5$.

### 1.5. Primitive $\lambda$-Roots

When dealing with composite odd values of $n$, we use the concept of a primitive $\lambda$-root [5, 6, 3]. On Carmichael's definition, an element from $\mathbb{U}_n$ is a *primitive $\lambda$-root* of $n$ if its order $\lambda(n)$ [Carmichael's function] is the maximum of the orders of all the elements from $\mathbb{U}_n$. We follow [3] by writing $\xi(n) = \phi(n)/\lambda(n)$.

Again as in [3], we describe a primitive $\lambda$-root $y$ of $n$ as *inward* if $y - 1 \in \mathbb{U}_n$; otherwise $y$ is *outward.* Also, we say that a unit $z$ is *negating* if $-1 \in \langle z \rangle$; otherwise, it is *non-negating.* If a primitive $\lambda$-root $y$ is inward and non-negating, we say that it is *strong.*

## 2. Cases Where $n$ is an Odd Prime Power

### 2.1. The Case With $n$ an Odd Prime

We now give some theorems that specify circumstances in which all or half of the members of $\mathbb{U}_n$ can be obtained from $\langle x \rangle \times \langle x+1 \rangle$ for some unit $x$, where $n$ is an odd prime power. For such $n$ in the range $0 < n < 300$, Table 2 gives all instances of $\langle x \rangle \times \langle x+1 \rangle$ providing all or half of $\mathbb{U}_n$. We start with $n$ prime.

**Theorem 1** *If $n$ is a prime satisfying $n \equiv 3 \pmod 8$, and $2$ is a primitive root of $n$, then $\mathbb{U}_n = \langle n-2 \rangle_m \times \langle n-1 \rangle_2$ where $m = (n-1)/2$.*

*Proof.* We have $m$ odd, and $n - 2 = 2^{m+1}$, so $n-2$ is a square in $\mathbb{Z}_n$, and $\text{ord}_n(n-2) = m$. Also $n - 1 = 2^m$, so $n-1$ is a non-square in $\mathbb{Z}_n$. □

**Theorem 2** *Let $n$ be a prime satisfying $n \equiv 3 \pmod 4$ and $n - 1 = 2ab$ where the odd integers $a$ and $b$ are co-prime (but not necessarily individually prime). Suppose that, for some $x \in \mathbb{U}_n$, we have*

$$\mathbb{U}_n = \langle x \rangle_a \times \langle x+1 \rangle_{2b}$$

*or*

$$\mathbb{U}_n = \langle x \rangle_{2a} \times \langle x+1 \rangle_b \ .$$

*Then we also have*

$$\mathbb{U}_n = \langle n-1-x \rangle_b \times \langle n-x \rangle_{2a}$$

*or*

$$\mathbb{U}_n = \langle n-1-x\rangle_{2b} \times \langle n-x\rangle_a \ ,$$

*respectively.*

*Proof.* Consider first the case $\mathbb{U}_n = \langle x\rangle_a \times \langle x+1\rangle_{2b}$. If $a = 1$ and $x = 1$, this case degenerates into Theorem 2.1. But, in general, as $n-x-1 = (x+1)^{b+1}$ where $b+1$ is even, we have $\mathrm{ord}_n(n-x-1) = 2b/\gcd(2b, b+1) = b$. Let $\theta = \mathrm{ord}_n(-x)$. Then $x^\theta = (-1)^\theta$, so $a \mid 2\theta$. Thus $a \mid \theta$, as $a$ is odd. But if $a = \theta$ then $x^a = -1$, which gives us a contradiction. So $\theta \geq 2a$. But $(-x)^{2a} = x^{2a} = 1$; so $\theta = 2a$. Finally, if $z \in \mathbb{U}_n$ then $z = x^u(x+1)^v$ for some $u$ and $v$, so that $z = (-x)^{u+a(u+v)}(-x-1)^v$. So $z \in \langle n-x\rangle \times \langle n-x-1\rangle$. Thus

$$\mathbb{U}_n = \langle n-x\rangle_{2a} \times \langle n-1-x\rangle_b \ .$$

The case $\mathbb{U}_n = \langle x\rangle_{2a} \times \langle x+1\rangle_b$ is dealt with similarly. □

**Note.** As indicated by Theorem 2.3 of [10] (see also [11]), particular interest attaches to the special case of the present Theorem 2 that has $\mathbb{U}_n = \langle x\rangle_a \times \langle x+1\rangle_{2b}$ and $n \equiv 3 \pmod{8\ [\text{not } 4]}$. The smallest prime $n$ for which this occurs is $n = 331$, with $\mathbb{U}_n = \langle 256\rangle_{15} \times \langle 257\rangle_{22} = \langle 74\rangle_{11} \times \langle 75\rangle_{30}$. The remaining such primes in the range $n < 1000$ are 443, 523, 547, 571, 659, 739, 827, 859 and 971.

**Theorem 3** *Let $n$ be a prime satisfying $n \equiv 5 \pmod 8$ and $(n-1)/2 = 2ab$ where the odd integers $a$ and $b$ are co-prime (but not nesessarily individually prime). Suppose that, for some $x \in \mathbb{U}_n$, precisely half of the elements of $\mathbb{U}_n$ are provided by*

$$\langle x\rangle_a \times \langle x+1\rangle_{2b}$$

*or*

$$\langle x\rangle_{2a} \times \langle x+1\rangle_b \ .$$

*Then the same half of the elements of $\mathbb{U}_n$ are also provided by*

$$\langle n-1-x\rangle_b \times \langle n-x\rangle_{2a}$$

*or*

$$\langle n-1-x\rangle_{2b} \times \langle n-x\rangle_a$$

*respectively.*

*Proof.* Exactly as for Theorem 2. □

**Theorem 4** *Let $n$ be a prime satisfying $n \equiv 5 \pmod 8$ and $n-1 = 4c$. If 2 is a primitive root of $n$, then there exists some element $x$ in $\mathbb{U}_n$ such that*

$$\mathbb{U}_n = \langle x\rangle_4 \times \langle x+1\rangle_c$$

*or*

$$\mathbb{U}_n = \langle x\rangle_c \times \langle x+1\rangle_4 \ .$$

*Proof.* We have $n = 4c + 1$ where $c \equiv 1$, 3, 5 or 7 (mod 8). We consider the four cases separately.

`Case (i).` $c \equiv 1 \pmod 8$. Let $y = 2^c$. Then $y^2 \equiv -1 \pmod n$, so $(y-1)^2 \equiv -2y \equiv 2^{3c+1} \pmod n$. Thus $y - 1 \equiv 2^{(3c+1)/2}$ or $2^{(7c+1)/2} \pmod n$.

If $y - 1 \equiv 2^{(7c+1)/2}$ then

$$\mathrm{ord}_n(y-1) = \mathrm{ord}_n(2^{(7c+1)/2}) = 4c/\gcd((7c+1)/2\,,\, 4c) = c\ .$$

Further, if $z \in \langle y\rangle \cap \langle y-1\rangle$ then $z \equiv 2^{ci} \equiv 2^{(7c+1)j/2}$ for some $i < 4$ and $j < c$, so $c \mid j$, whence $j = 0$ and $z = 1$. Thus $\langle y\rangle \cap \langle y-1\rangle = \{1\}$, and the result follows with $x = y - 1$.

Contrariwise, if $y - 1 \equiv 2^{(3c+1)/2}$, let $x = -y$. Then $x = 2^{3c}$ and $x + 1 = -(y-1) = 2^{(7c+1)/2}$ where $x$ and $x+1$ have orders 4 and $c$ respectively. Then $\langle x\rangle \cap \langle x+1\rangle = \{1\}$ and the result follows.

`Case (ii).` $c \equiv 3 \pmod 8$. Take $y = 2^{3c}$ so that $y - 1 \equiv 2^{(c+1)/2}$ or $2^{(5c+1)/2}$. If $y-1 \equiv 2^{(c+1)/2}$ take $x = -y = 2^c$ to obtain $\mathbb{U}_n = \langle x\rangle_4 \times \langle x+1\rangle_c$. If $y-1 \equiv 2^{(5c+1)/2}$ we have $\mathbb{U}_n = \langle y-1\rangle_c \times \langle y\rangle_4$, so take $x = y - 1$.

`Case (iii).` $c \equiv 5 \pmod 8$. Take $y = 2^c$ so that $y - 1 \equiv 2^{(3c+1)/2}$ or $2^{(7c+1)/2}$. Take $x = y - 1$ or $x = -y$ respectively, so that the allocation is the other way round from in (i).

`Case (iv).` $c \equiv 7 \pmod 8$. Take $y = 2^{3c}$ so that $y - 1 \equiv 2^{(c+1)/2}$ or $2^{(5c+1)/2}$. Take $x = y - 1$ or $x = -y$ respectively. □

**Examples.**

`Case (i).` $n = 37$, $c = 9$. Take $y = 2^9 \equiv 31$ whence $y - 1 = 30 \equiv 2^{(3c+1)/2}$, so use $x = -y = 6$ to obtain $\mathbb{U}_{37} = \langle 6\rangle_4 \times \langle 7\rangle_9$.

`Case (iv).` $n = 29$, $c = 7$. Take $y = 2^{21} \equiv 17$ whence $y - 1 = 16 \equiv 2^{(c+1)/2}$, so use $x = y - 1 = 16$ to obtain $\mathbb{U}_{29} = \langle 16\rangle_7 \times \langle 17\rangle_4$.

**Theorem 5** *Let $n$ be a prime satisfying $n \equiv 9 \pmod{16}$ and $n-1 = 8c$. If $\mathrm{ord}_n(2) = (n-1)/2$, then there exists some element $x$ in $\mathbb{U}_n$ such that precisely half of the elements in $\mathbb{U}_n$ are provided by*

$$\langle x\rangle_4 \times \langle x+1\rangle_c\ .$$

*No two members of this last set are the negatives of one another, modulo $n$.*

*Proof.* As for Theorem 4; here again $\mathrm{ord}_n(2) = 4c$. Now $x$ and $x + 1$ are both squares in $\mathbb{Z}_n$. □

**Theorem 6** *Let $n$ be a prime satisfying $n \equiv 7$ or $13 \pmod{18}$. Suppose that there exists an element $x$ from $\mathbb{U}_n$ such that $x^2 + 3x + 3 \equiv 0 \pmod n$ with $\mathrm{ord}_n(x) =$*

$(n-1)/3$. *Then* $\mathrm{ord}_n(x+1) = 3$ *and*

$$\mathbb{U}_n = \langle x \rangle_{(n-1)/3} \times \langle x+1 \rangle_3 \ .$$

*Proof.* Clearly $(x+1)^3 \equiv 1 \pmod{n}$, so $\mathrm{ord}_n(x+1) = 3$. To show that $\langle x \rangle \cap \langle x+1 \rangle = \{1\}$, suppose that $x+1 \equiv x^j \pmod{n}$ for some $j$ with $0 < j < (n-1)/3$. Then $1 \equiv (x+1)^3 \equiv x^{3j} \pmod{n}$, so that $3j = (n-1)/3$ or $2(n-1)/3$. But if $n \equiv 7$ or $13 \pmod{18}$, the quantity $(n-1)/9$ is not an integer, so the supposition must be false. □

**Note.** The solutions $x_1$ and $x_2$ of the quadratic congruence $x^2 + 3x + 3 \equiv 0 \pmod{n}$ are given by $x = 2^{-1}(\pm\sqrt{-3} - 3)$ with $x_1 + x_2 \equiv -3$ and $x_1 x_2 \equiv 3 \pmod{n}$. But $\mathrm{ord}_n(x) = (n-1)/3$ cannot be satisfied by **both** $x_1$ and $x_2$. [Suppose that $\mathrm{ord}_n(x_1) = (n-1)/3$. Then, as $x_1 x_2 \equiv 3 \pmod{n}$, we have $x_2^{(n-1)/3} \equiv 3^{(n-1)/3} \pmod{n}$. Thus, if we also have $\mathrm{ord}_n(x_2) = (n-1)/3$, then $3^{(n-1)/3} \equiv 1 \pmod{n}$. But $x_1^2 \equiv -3(x_1+1)$, whence, as $(n-1)/3$ is even, $x_1^{2(n-1)/3} \equiv 3^{(n-1)/3}(x_1+1)^{(n-1)/3}$, so that $(x_1+1)^{(n-1)/3} \equiv 1 \pmod{n}$. But $\mathrm{ord}_n(x_1+1) = 3$, whence $3 \mid (n-1)/3$, so that $9 \mid n-1$, which gives a contradiction.

**Examples.** In the range $0 < n < 300$, the conditions of Theorem 6 are satisfied only by $(n, x) = (13, 8)$, $(97, 34)$, $(139, 95)$, $(223, 182)$, $(229, 93)$, $(241, 224)$, $(277, 159)$ and $(283, 43)$.

**Theorem 7** *Let* $n$ *be a prime satisfying* $n \equiv 7$ *or* $13 \pmod{18}$. *Suppose that there exists an element* $x$ *from* $\mathbb{U}_n$ *such that* $x^2 + 3x + 3 \equiv 0 \pmod{n}$ *with* $\mathrm{ord}_n(x) = (n-1)/6$. *Then* $\mathrm{ord}_n(x+1) = 3$*, and half of the members of* $\mathbb{U}_n$ *are provided by*

$$\langle x \rangle_{(n-1)/6} \times \langle x+1 \rangle_3 \ ,$$

*which does not contain* $-1 \pmod{n}$.

*Proof.* Similar to the proof of Theorem 6. As for Theorem 6, there can be no more than one value $x$ satisfying the specified conditions. □

**Examples.** In the range $0 < n < 300$, we have $(n, x) = (7, 1)$, $(31, 4)$, $(43, 35)$, $(79, 22)$ and $(211, 13)$.

### 2.2. Theorems for $n = p^m$ With $m > 1$

We now consider values $n$ that satisfy $n = p^m$ $(m > 1)$ where $p$ is an odd prime; for this we need the concept of a Wieferich prime. A prime $p$ is said to be a *Wieferich prime* [13, 7, 2] if $\mathrm{ord}_n(2) = \mathrm{ord}_p(2)$ where $n = p^2$. The only known Wieferich primes are $p = 1093$, for which $\mathrm{ord}_n(2) = \mathrm{ord}_p(2) = (p-1)/3$, and $p = 3511$, for which $\mathrm{ord}_n(2) = \mathrm{ord}_p(2) = (p-1)/2$. Thus no Wieferich prime is known that has 2 as a primitive root; whether such a value exists is an open question.

**Theorem 8** *Let $n = p^2$ where $p$ is any prime, other than a Wieferich prime, that has 2 as a primitive root. Then*

$$\mathbb{U}_n = \langle y-1\rangle_p \times \langle y\rangle_{p-1}$$

*where $y \equiv 2^p \pmod{p^2}$.*

*Proof.* As $p$ is not a Wieferich prime, $y \neq 2$. For some $i$, we have $(y-1)^p = (1+ip)^p \equiv 1 \pmod{p^2}$. So we have $\mathrm{ord}_n(y-1) = p$.

We now show that $\langle y-1\rangle \times \langle y\rangle = \{1\}$. As 2 is a primitive root of both $p$ and $p^2$, we have $y = 2^{1+j(p-1)}$ and $y-1 = 2^{h(p-1)}$ for some $j, h$. Suppose that $y^c \equiv (y-1)^d \pmod{p^2}$ for some $c$ and $d$ with $0 \leq c < p-1$. Then $c + cj(p-1) \equiv dh(p-1) \pmod{p(p-1)}$. Thus $(p-1) \mid c$, whence $c = 0$ and $y^c = 1$. □

**Theorem 9** *Let $n = p^2$ where $p$ is a prime such that $\mathrm{ord}_p(2) = (p-1)/2$ and $p$ is not a Wieferich prime. Take $y \equiv 2^p \pmod{p^2}$. Then the set*

$$\langle y-1\rangle_p \times \langle y\rangle_{(p-1)/2}$$

*comprises precisely half of the elements of $\mathbb{U}_n$. This set excludes $-1$ if $p \equiv 3 \pmod 4$.*

*Proof.* The main part of the proof is similar to the proof of Theorem 8. Then, for $p \equiv 3 \pmod 4$, suppose that $(y-1)^u y^v \equiv -1 \pmod{p^2}$. Now, as $y \equiv 2 \pmod p$, we have $2^v \equiv -1 \pmod p$, so $-1$ is a power of 2. But $\mathrm{ord}_p(2) = (p-1)/2$, which is odd, so 2 is a square in $\mathbb{Z}_p$, which implies that $-1$ is a square in $\mathbb{Z}_p$, which is false when $p \equiv 3 \pmod 4$. □

**Theorem 10** *Let $n = p^m$ $(m \geq 2)$ where $p$ is any prime, other than a Wieferich prime, that has 2 as a primitive root. Take $y \equiv 2^{n/p} \pmod{p^m}$. Then*

$$\mathbb{U}_n = \langle y-1\rangle_{n/p} \times \langle y\rangle_{p-1} \ .$$

*Proof.* As $y = 2 + ip + jp^2$ for some $i$ and $j$ with $0 < i \leq p-1$, we have

$$(y-1)^{p^{m-1}} = (1+ip+jp^2)^{p^{m-1}} \equiv 1 \pmod{p^m} \ .$$

But

$$(y-1)^{p^{m-2}} = (1+ip+jp^2)^{p^{m-2}} \equiv 1 + ip^{m-1} \not\equiv 1 \pmod{p^m} \ ,$$

so $\mathrm{ord}_{p^m}(y-1) = p^{m-1}$.

The result $\langle y-1\rangle \cap \langle y\rangle = \{1\}$ follows as in previous proofs. □

### 2.3. Lifts

To proceed further in obtaining decompositions $\langle x \rangle \times \langle x+1 \rangle$ of $\mathbb{U}_n$ where $n$ is a power of a prime $p$, we introduce the concept of a *lift*, which has been very fruitful in related studies [4, 12]. We do not now do this in full generality, but start simply with lifts from $p$ to $p^2$.

Suppose that we have a decomposition $\langle x \rangle_a \times \langle x+1 \rangle_b$ for $\mathbb{U}_p$ where $p$ is an odd prime. Take $n = p^2$. Then, for some values $i^*$ and $j^*$ from $\{0, 1, \ldots, p-1\}$, we have

$$\mathrm{ord}_n(x+ip) \quad = \quad \begin{cases} a, & i = i^* \\ ap, & i \in \{0,1,\ldots,p-1\} \setminus \{i^*\} \end{cases}$$

and

$$\mathrm{ord}_n(x+1+jp) \quad = \quad \begin{cases} b, & j = j^* \\ bp, & j \in \{0,1,\ldots,p-1\} \setminus \{j^*\} \end{cases} \quad .$$

Thus, unless $i^* = j^*$, we have the following two decompositions of $\mathbb{U}_n$:

$$\langle x + i^*p \rangle_a \times \langle x+1+i^*p \rangle_{bp}$$

and

$$\langle x + j^*p \rangle_{ap} \times \langle x+1+j^*p \rangle_b \ .$$

We refer to these variously as *lifts* of the decomposition $\langle x \rangle_a \times \langle x+1 \rangle_b$ for $\mathbb{U}_p$, and as *lifts* from $p$ to $n$. Table 1 can be used to check that, for odd primes $p$ less than 300, there is no instance of such a lift failing as a result of having $i^* = j^*$.

If 2 is a primitive root of a prime $p$ that is not a Wieferich prime, and $n = p^2$, we can similarly lift the degenerate decomposition $\langle 1 \rangle_1 \times \langle 2 \rangle_{p-1}$ for $\mathbb{U}_p$ to the decomposition $\langle 2^p - 1 \rangle_p \times \langle 2^p \rangle_{p-1}$ for $\mathbb{U}_n$, as shown in Theorem 8.

## 3. Some Basic Results, $n$ Composite

### 3.1. A Lemma

We start with a lemma giving an important restriction on the orders $a$ and $b$ when

$$\mathbb{U}_n = \langle x \rangle_a \times \langle x+1 \rangle_b$$

for a (necessarily odd) composite value $n$.

**Lemma 11** *If, for $n$ composite and odd, we have*

$$\mathbb{U}_n = \langle x \rangle_a \times \langle x+1 \rangle_b$$

*for some unit $x$, then $\xi(n)$ is a factor of both $a$ and $b$.*

*Proof.* $\lambda(n)\xi(n) = \phi(n) = ab = \gcd(a,b) \cdot \mathrm{lcm}(a,b)$. However, $\mathrm{lcm}(a,b) \mid \lambda(n)$, so $\xi(n) \mid \gcd(a,b)$. □

### 3.2. Three Simple Theorems

We now come to some Theorems that apply, in particular, to odd composite integers $n$ with $\xi(n) = 2$. Such integers are of the form $p^i q^j$ $(i \geq 1, j \geq 1)$ where $p$ and $q$ are distinct odd primes. For such integers in the range $0 < n < 300$, Table 2 gives all instances of $\langle x \rangle \times \langle x+1 \rangle$ providing all or half of $\mathbb{U}_n$. Table 3 similarly covers values of $n$ with $\xi(n) \geq 4$. Our first three theorems are elementary.

**Theorem 12** *Let $n$ be a positive integer satisfying $\xi(n) = 2$. If $2$ is a strong primitive $\lambda$-root of $n$, then*

$$\mathbb{U}_n = \langle n-2 \rangle_{\phi(n)/2} \times \langle n-1 \rangle_2 \ .$$

*Proof.* As 2 is a non-negating primitive $\lambda$-root of $n$, and $\lambda(n) = \phi(n)/2$ is even, the unit $n-2$ is a primitive $\lambda$-root of $n$. The result follows, as $n-1 \notin \langle n-2 \rangle$ . □

**Theorem 13** *Let $n$ be a positive integer satisfying $\xi(n) = 2$ or $4$. If $n-2$ is a non-negating unit of $\mathbb{Z}_n$ with $\mathrm{ord}_n(n-2) = \phi(n)/4$, then*

$$\langle n-2 \rangle_{\phi(n)/4} \times \langle n-1 \rangle_2$$

*comprises precisely half of the members of $\mathbb{U}_n$.*

*Proof.* As $n-2$ is non-negating, $n-1 \notin \langle n-2 \rangle$ . □

**Theorem 14** *Let $n$ be a positive integer such that $\xi(n) = 2$ and $\phi(n)/4$ is odd. If $2$ is a negating primitive $\lambda$-root of $n$, then*

$$\langle n-2 \rangle_{\phi(n)/4} \times \langle n-1 \rangle_2$$

*comprises precisely half of the members of $\mathbb{U}_n$ and is precisely $\langle 2 \rangle$.*

*Proof.* The conditions of this theorem imply the conditions of Theorem 13 (but not *vice versa*). □

### 3.3. The Case $n = p\nu$ With $p$ Prime, $\nu$ a Prime Power

Our next three theorems relate to $n$-values of the form $n = p\nu$ where $p$ is an odd prime and $\nu$ is an odd prime power. In the terminology of lifts (see Section 2.2 above), these theorems concern lifts from $\nu$ to $n$.

**Theorem 15** *Let $\nu = q^i$ $(i \geq 1)$ where $q$ is an odd prime. Suppose that there is an element $x$, with $1 < x < \nu - 2$, such that*

$$\mathbb{U}_\nu = \langle x \rangle_a \times \langle x+1 \rangle_b \pmod{\nu}$$

*for some integers $a$ and $b$ that are mutually prime and of opposite parity. Let $p$ be an odd prime, $p \neq q$, such that* $\gcd(b, (p-1)/2) = 1$ *and* $p \equiv 1$ *or* $3 \pmod 4$ *according as the integer $a$ is even or odd. Suppose that there exists an integer $k$, $0 \le k \le p-1$, such that* $\operatorname{ord}_p(x+k\nu) \mid a$ *and* $\operatorname{ord}_p(x+k\nu+1) = p-1$ *or* $(p-1)/2$. *Then, with $n = p\nu$,*

$$\langle x+k\nu\rangle_a \times \langle x+k\nu+1\rangle_{b(p-1)} \pmod n$$

*gives the whole of $\mathbb{U}_n$ if* $p \equiv 1 \pmod 4$ *and* $\operatorname{ord}_p(x+k\nu+1) = p-1$, *whereas*

$$\langle x+k\nu\rangle_a \times \langle x+k\nu+1\rangle_{b(p-1)/2} \pmod n$$

*gives half of $\mathbb{U}_n$ otherwise. If* $p \equiv 3 \pmod 4$, *this set of half of the elements of $\mathbb{U}_n$ excludes $-1$.*

*Proof.* We have

$$\begin{aligned}\operatorname{ord}_n(x+k\nu) &= \operatorname{lcm}(\operatorname{ord}_p(x+k\nu), \operatorname{ord}_\nu(x)) \\ &= \operatorname{lcm}(\operatorname{ord}_p(x+k\nu), a) \ = \ a\end{aligned}$$

and, except when $p \equiv 1 \pmod 4$ and $\operatorname{ord}_p(x+k\nu+1) = p-1$, we have

$$\begin{aligned}\operatorname{ord}_n(x+k\nu+1) &= \operatorname{lcm}(\operatorname{ord}_p(x+k\nu+1), \operatorname{ord}_\nu(x+1)) \\ &= \operatorname{lcm}((p-1)/2, b) \ = \ b(p-1)/2 \ .\end{aligned}$$

So the product has $ab(p-1)/2 = \phi(n)\,/\,2$ elements provided that it is direct. To show that it is indeed direct, suppose that

$$(x+k\nu)^\alpha \equiv (x+k\nu+1)^\beta \pmod n \ ,$$

where $0 \le \alpha < a$ and $0 \le \beta < b(p-1)/2$. Then $x^\alpha \equiv (x+1)^\beta \pmod \nu$, whence $x^\alpha = 1$ and $\alpha = 0$, so that $(x+k\nu)^\alpha \equiv 1 \pmod n$.

When $p \equiv 1 \pmod 4$ and $\operatorname{ord}_p(x+k\nu+1) = p-1$, we have $\operatorname{ord}_n(x+k\nu+1) = \operatorname{lcm}(p-1, b) = b(p-1)$.

Finally, suppose that $p \equiv 3 \pmod 4$, so that $a$ is odd. If $-1 \in \langle x+k\nu\rangle \times \langle x+k\nu+1\rangle$ then $(x+k\nu)^\lambda \equiv -(x+k\nu+1)^\mu \pmod n$ for some integers $\lambda$ and $\mu$ with $0 \le \lambda < a$. But then $(x+k\nu)^{2\lambda} \equiv (x+k\nu+1)^{2\mu} \pmod n$, and so $(x+k\nu)^{2\lambda} \equiv 1$. Thus $2\lambda = 0$ or $a$, whence $\lambda = 0$ as $a$ is odd. Thus $(x+k\nu+1)^\mu \equiv -1 \pmod n$. But then $(x+k\nu+1)^\mu \equiv -1 \pmod p$, which is impossible as $\operatorname{ord}_p(x+k\nu+1)$ is odd. □

**Note.** In the range $0 < n < 300$, the conditions of Theorem 15 are satisfied by the following parameter sets:

| $n$ | $p$ | $\nu$ | $x$ | $a$ | $b$ | $k$ | $x{+}k\nu$ | $\xi(n)$ |
|---|---|---|---|---|---|---|---|---|
| Whole of $\mathbb{U}_n$: | | | | | | | | |
| 65 | 5 | 13 | 8 | 4 | 3 | 1 or 3 | 21 or 47 | 4 |
| 185 | 5 | 37 | 6 | 4 | 9 | 0 or 3 | 6 or 117 | 4 |
| 265 | 5 | 53 | 23 | 4 | 13 | 1 or 3 | 76 or 182 | 4 |
| Half of $\mathbb{U}_n$: | | | | | | | | |
| 65 | 5 | 13 | 8 | 4 | 3 | 0 | 8 | 4 |
| 75 | 3 | 25 | 6 | 5 | 4 | 1 | 31 | 2 |
| 87 | 3 | 29 | 16 | 7 | 4 | 0 | 16 | 2 |
| 123 | 3 | 41 | 37 | 5 | 8 | 0 | 37 | 2 |
| 175 | 7 | 25 | 6 | 5 | 4 | 4 | 106 | 2 |
| 183 | 3 | 61 | 20 | 5 | 12 | 2 | 142 | 2 |
| 185 | 5 | 37 | 6 | 4 | 9 | 1 | 43 | 4 |
| 203 | 7 | 29 | 16 | 7 | 4 | 6 | 190 | 2 |
| 213 | 3 | 71 | 45 | 7 | 10 | 2 | 187 | 2 |
| | | | 25 | 5 | 14 | 0 | 25 | |
| 265 | 5 | 53 | 23 | 4 | 13 | 0 | 23 | 4 |
| 275 | 11 | 25 | 6 | 5 | 4 | 2 or 10 | 56* or 256 | 10 |
| 287 | 7 | 41 | 37 | 5 | 8 | 1 | 78 | 2 |

* this value arises also from Theorem 6.1

**Example.** $(n,p,\nu) = (87,3,29)$. We have $\mathbb{U}_{29} = \langle 16\rangle_7 \times \langle 17\rangle_4 \pmod{29}$, and can take $k = 0$ to obtain precisely half of the elements of $\mathbb{U}_{87}$ from $\langle 16\rangle_7 \times \langle 17\rangle_4 \pmod{87}$.

**Theorem 16** *Let $\nu = q^i$ $(i \geq 1)$ where $q$ is a prime satisfying $q \equiv 3 \pmod 4$. Suppose that there is an element $x$, with $1 < x < \nu - 2$, such that half of the elements of $\mathbb{U}_n$ are given by $\langle x\rangle_a \times \langle x+1\rangle_b \pmod{\nu}$ for some odd integers $a$ and $b$ that are mutually prime. Let $p$ be an odd prime, $p \neq q$, such that $\gcd(b, p-1) = 1$. Suppose that there exists an integer $k$, $0 \leq k \leq p-1$, such that $\mathrm{ord}_p(x + k\nu) \mid a$ and $\mathrm{ord}_p(x + k\nu + 1) = p - 1$. Then, with $n = p\nu$, precisely half of the elements of $\mathbb{U}_n$ are given by $\langle x + k\nu\rangle_a \times \langle x + k\nu + 1\rangle_{b(p-1)} \pmod{n}$ . This set of half of the elements of $\mathbb{U}_n$ excludes $-1$. If $2$ is a primitive root of $p$, a value of $k$ always exists, namely the value such that $x + k\nu \equiv 1 \pmod{p}$.*

*Proof.* Similar to that of Theorem 15. Here $\mathrm{ord}_n(x + k\nu + 1) = \mathrm{lcm}(p-1, b) = b(p-1)$ . With $\mu$ as in the proof of Theorem 15, we now have $(x + k\nu + 1)^{2\mu} \equiv 1 \pmod{n}$, so $2\mu$ is a multiple of $b(p-1)$, *i.e.* $\mu$ is a multiple of $b(p-1)/2$ where $0 < \mu < b(p-1)$. Thus $\mu = b(p-1)/2$ and $(x+1)^{b(p-1)/2} \equiv -1 \pmod{\nu}$. But $(x+1)^b \equiv 1 \pmod{\nu}$, so $(x+1)^{b(p-1)/2} \equiv 1$, not $-1 \pmod{\nu}$, which gives us a contradiction.

Taking $k$ so that $x + k\nu \equiv 1 \pmod{p}$ gives $\mathrm{ord}_p(x + k\nu) = \mathrm{ord}_p(1) = 1$ and $\mathrm{ord}_p(x + k\nu + 1) = \mathrm{ord}_p(2) = p - 1$ if 2 is a primitive root of $p$. □

**Note.** In the range $0 < n < 300$, the conditions of Theorem 16 are satisfied by the following parameter sets:

| $n$ | $p$ | $\nu$ | $x$ | $a$ | $b$ | $k$ | $x+k\nu$ | $\xi(n)$ |
|---:|---:|---:|---:|---:|---:|---:|---:|---:|
| 93 | 3 | 31 | 4 | 5 | 3 | 0 | 4 | 2 |
| 129 | 3 | 43 | 35 | 7 | 3 | 2 | 121 | 2 |
| 147 | 3 | 49 | 29 | 7 | 3 | 2 | 127 | 2 |
| 155 | 5 | 31 | 4 | 5 | 3 | 2 | 66 | 2 |
| 215 | 5 | 43 | 35 | 7 | 3 | 2 | 121 | 2 |
| 237 | 3 | 79 | 22 | 13 | 3 | 0 | 22 | 2 |
| 245 | 5 | 49 | 29 | 7 | 3 | 3 | 176 | 2 |

**Example.** $(n, p, \nu) = (93, 3, 31)$. Half of the elements of $\mathbb{U}_{31}$ are in $\langle 4\rangle_5 \times \langle 5\rangle_3 \pmod{31}$, and we can take $k = 0$ to obtain precisely half of the elements of $\mathbb{U}_{93}$ from $\langle 4\rangle_5 \times \langle 5\rangle_6 \pmod{93}$.

**Theorem 17** *Let $n = 9p$ where $p$ is a prime $(p > 3)$ for which $\mathrm{ord}_p(2) = p - 1$ or $(p - 1)/2$, but $p \not\equiv 17 \pmod{24}$. Then there exists at least one unit $x$ in $\mathbb{U}_n$ such that precisely half of the elements of $\mathbb{U}_n$ are given by $\langle x\rangle_3 \times \langle x+1\rangle_{p-1}$ . In each case we can take $x = 3p + 1$. If $p \equiv 7$, $13$ or $19 \pmod{24}$ we can also take $x = 6p + 1$. If $p \equiv 5$, $7$, $13$ or $23 \pmod{24}$, $\langle x\rangle \times \langle x + 1\rangle$ excludes $-1 \pmod{n}$.*

*Proof.* The possibility $\mathrm{ord}_p(2) = p - 1$ can occur only if 2 is a non-square in $\mathbb{Z}_n$, *i.e.* when $p \equiv \pm 3 \pmod{8}$, whereas $\mathrm{ord}_p(2) = (p - 1)/2$ only if 2 is a square in $\mathbb{Z}_n$, *i.e.* when $p \equiv \pm 1 \pmod{8}$.

Straightforward argument shows that $\mathrm{ord}_p(x) = 3$ in each of the cases $p \equiv 1$, 5, 7, 11, 13, 19 and 23 (mod 24). To illustrate the rest of the proof for each of these, we present it for just two of them, namely (i) $p \equiv 5$ and (ii) $p \equiv 7 \pmod{24}$.

Case (i). Let $p = 24u+5$, with $\mathrm{ord}_p(2) = p-1$. Let $x = 3p+1 = 72u+16$. Then $x + 1 = 72u + 17$, so that $\mathrm{ord}_9(x + 1) = \mathrm{ord}_9(-1) = 2$ and $\mathrm{ord}_p(x + 1) = \mathrm{ord}_p(2) = p - 1$, giving $\mathrm{ord}_{9p}(x + 1) = \mathrm{lcm}(2,\, p - 1) = p - 1$. So the required result follows if we can show that $\langle x\rangle \cap \langle x + 1\rangle = \{1\}$. As $\mathrm{ord}_{9p}(x) = 3$ it suffices to suppose that $x \equiv (x + 1)^m \pmod{9p}$ for some $m$ with $0 < m < p - 1$. But then we would have $1 \equiv 2^m \pmod{p}$, contradicting the fact that $\mathrm{ord}_p(2) = p - 1$. Thus we can indeed take $x = 3p + 1$.

Now, if we take $y = 6p + 1$ we have $y + 1 = 144u + 32$, whence $\mathrm{ord}_9(y + 1)$ $= \mathrm{ord}_9(5) = 6$ and $\mathrm{ord}_p(y+1) = \mathrm{ord}_p(2) = p-1$. Thus $\mathrm{ord}_{9p}(y+1) = \mathrm{lcm}(6,\, p-1) = 3(p - 1) \neq p - 1$, so we cannot take $x = y$.

Case (ii). Now let $p = 24u+7$, with $\mathrm{ord}_p(2) = (p-1)/2$. Let $x = 3p+1 = 72u+22$. Then $\mathrm{ord}_{9p}(x + 1) = \mathrm{lcm}(6,\, (p - 1)/2) = \mathrm{lcm}(12u + 3,\, 6) = p - 1$. Suppose that

$x \equiv (x+1)^m \pmod{9p}$ for some $m$ with $0 < m < p-1$. The $2^m \equiv 1 \pmod{p}$ and so $m = (p-1)/2$. Thus we have $4 \equiv 5^{12u+3} \equiv -1 \pmod{9}$, which is a contradiction. So $\langle x \rangle \cap \langle x+1 \rangle = \{1\}$.

If we take $y = 6p+1$ we obtain $y+1 \equiv -1 \pmod{9}$, so $\mathrm{ord}_9(y+1) = 2$. So $\mathrm{ord}_{9p}(y+1) = \mathrm{lcm}(12u+3, 2) = p-1$, and the result follows as before.

We now show why we must exclude the case $p \equiv 17 \pmod{24}$. If we take $p = 24u+17$ and $x = 3p+1$ we must have $\mathrm{ord}_p(2) = (p-1)/2$ and $x = 72u+52$. Then $\mathrm{ord}_9(x+1) = \mathrm{ord}_9(-1) = 2$ and $\mathrm{ord}_p(x+1) = \mathrm{ord}_p(2) = (p-1)/2$, so that $\mathrm{ord}_{9p}(x+1) = \mathrm{lcm}(2, (p-1)/2) \neq p-1$ as $(p-1)/2$ is even. □

**Note.** In the range $0 < n < 300$, the conditions of Theorem 17 are satisfied as in this table:

| $n$ | $p$ | $x$ | $\xi(n)$ |
|---|---|---|---|
| 45 | 5 | 16 | 2 |
| 63 | 7 | 22 or 43 | 6 |
| 99 | 11 | 34 | 2 |
| 117 | 13 | 40 or 79 | 6 |
| 171 | 19 | 58 or 115 | 6 |
| 207 | 23 | 70 | 2 |
| 261 | 29 | 88 | 2 |

### 3.4. The Case $n = pq$ With $p$ and $q$ Both Prime

Our next three theorems relate to $n$-values of the form $n = pq$ where $p$ and $q$ are distinct odd primes.

**Theorem 18** *Let $n = pq$ where $p$ and $q$ are primes such that $p \equiv 7 \pmod{8}$ with $\mathrm{ord}_p(2) = (p-1)/2$, and $q \equiv 5 \pmod{8}$ with 2 a primitive root of $q$. Then $\mathbb{U}_n = \langle x \rangle_{p-1} \times \langle x+1 \rangle_{q-1}$, where $x$ is the unique unit with $x \equiv -2 \pmod{p}$ and $x \equiv 1 \pmod{q}$.*

*Proof.* As the unit 2 is a square, modulo $p$, the unit $-2$ is a non-square and so $\mathrm{ord}_p(-2)$ is even. But if $(-2)^{2k} \equiv 1 \pmod{p}$, then $2^{2k} \equiv 1 \pmod{p}$ and so $2k$ is a multiple of $(p-1)/2$. But $(p-1)/2$ is odd, so $2k = p-1$. Thus $\mathrm{ord}_p(-2) = p-1$, and so $\mathrm{ord}_{pq}(x) = \mathrm{lcm}(\mathrm{ord}_p(-2), \mathrm{ord}_q(1)) = \mathrm{lcm}(p-1, 1) = p-1$.

Also $\mathrm{ord}_{pq}(x+1) = \mathrm{lcm}(\mathrm{ord}_p(-1), \mathrm{ord}_q(2)) = \mathrm{lcm}(2, q-1) = q-1$.

It remains to show that $\langle x \rangle \cap \langle x+1 \rangle = \{1\}$. Suppose that $x^\alpha \in \langle x+1 \rangle$ for some $\alpha$ satisfying $0 \leq \alpha < p-1$. Then $x^\alpha \equiv (x+1)^\beta \pmod{pq}$ for some $\beta$. Thus $2^\beta \equiv 1 \pmod{q}$, so $\beta$ is even. But the congruence $x^\alpha \equiv (x+1)^\beta \pmod{p}$ gives $(-2)^\alpha \equiv 1 \pmod{p}$, so $\alpha$ is a multiple of $p-1$. Thus $\alpha = 0$ and $\langle x \rangle \cap \langle x+1 \rangle = \{1\}$. □

**Examples.** In the range $0 < n < 300$ the examples that arise from Theorem 18 are as follows:

| $n$ | $p$ | $q$ | $x$ | $\xi(n)$ |
|---|---|---|---|---|
| 35 | 7 | 5 | 26 | 2 |
| 91 | 7 | 13 | 40 | 6 |
| 115 | 23 | 5 | 21 | 2 |
| 203 | 7 | 29 | 117 | 2 |
| 235 | 47 | 5 | 186 | 2 |
| 259 | 7 | 37 | 75 | 6 |
| 299 | 23 | 13 | 274 | 2 |

**Theorem 19** *Let $n = pq$ where $p$ and $q$ are primes such that $p \equiv 7 \pmod 8$ with $\mathrm{ord}_p(2) = (p-1)/2$, and $q \equiv 3 \pmod 8$ with 2 a primitive root of $q$. Then $\mathbb{U}_n = \langle x\rangle_{p-1} \times \langle x+1\rangle_{q-1}$, where $x$ is the unique unit with $x \equiv -2 \pmod p$ and $x \equiv 1 \pmod q$. Also, with the same $x$, half of $\mathbb{U}_n$ is given by $\langle\ -(x+1)\ \rangle_{(q-1)/2} \times \langle\ -x\ \rangle_{p-1}$ , which does not include $-1 \pmod n$.*

*Proof.* The first part is as in the proof of Theorem 18. Now we have $\mathrm{ord}_{pq}(-x) = \mathrm{lcm}(\mathrm{ord}_p(2), \mathrm{ord}_q(-1)) = \mathrm{lcm}((p-1)/2, 2) = p-1$. Also, since $\mathrm{ord}_q(-2) = \mathrm{ord}_q(2^{(q+1)/2}) = (q-1)/2$, we have $\mathrm{ord}_{pq}(-(x+1)) = \mathrm{lcm}(\mathrm{ord}_p(1), \mathrm{ord}_q(-2)) = (q-1)/2$.

To show that $\langle\ -(x+1)\ \rangle \cap \langle\ -x\ \rangle = \{1\}$, suppose that $(-(x+1))^\alpha \equiv (-x)^\beta \pmod{pq}$ for some $\alpha$ and $\beta$ with $0 \le \beta < p-1$. Then $2^\beta \equiv 1 \pmod p$, so that $\beta = (p-1)/2$. Thus $(-2)^\alpha \equiv (-1)^\beta \equiv -1 \pmod q$, which is impossible as $\mathrm{ord}_q(-2)$ is odd.

Thus $\langle\ -(x+1)\ \rangle \cap \langle\ -x\ \rangle$ gives half of $\mathbb{U}_n$. Finally we show that $-1 \notin \langle\ -(x+1)\ \rangle \times \langle\ -x\ \rangle$. Suppose that $(-(x+1))^a x^b \equiv -1 \pmod{pq}$ for some $a$ and $b$. Then $2^b \equiv -1 \pmod p$, which gives a contradiction as $\mathrm{ord}_p(2)$ is odd. □

**Examples.** In the range $0 < n < 300$ the examples that arise from Theorem 19 are as follows, where we include the trivial examples with $q = 3$ and therefore $x = n-2$:

| $n$ | $p$ | $q$ | $x$ | $\xi(n)$ |
|---|---|---|---|---|
| 21 | 7 | 3 | 19 | 2 |
| 69 | 23 | 3 | 67 | 2 |
| 77 | 7 | 11 | 12 | 2 |
| 133 | 7 | 19 | 96 | 6 |
| 141 | 47 | 3 | 139 | 2 |
| 213 | 71 | 3 | 211 | 2 |
| 237 | 79 | 3 | 235 | 2 |
| 253 | 23 | 11 | 67 | 2 |

**Theorem 20** *Let $n = pq$ where $p$ and $q$ are primes such that $p \equiv 5 \pmod 8$ with $2$ a primitive root of $p$, and $q \equiv 3 \pmod 8$ with $2$ also a primitive root of $q$. Then*

$$\mathbb{U}_n = \langle x \rangle_{p-1} \times \langle x+1 \rangle_{q-1}$$

*where $x$ is the unique unit with $x \equiv -2 \pmod p$ and $x \equiv 1 \pmod q$. Also, with the same $x$, half of $\mathbb{U}_n$ is given by*

$$\langle\ -(x+1)\ \rangle_{(q-1)/2} \times \langle\ -x\ \rangle_{p-1}\ ,$$

*which does not include $-1 \pmod n$.*

*Proof.* As $\gcd(p-1,\,(p+1)/2) = 1$, we have $\text{ord}_{pq}(x) = \text{lcm}(\text{ord}_p(-2),\, \text{ord}_q(1))$ $= \text{lcm}(p-1,\, 1) = p-1$. Similarly $\text{ord}_{pq}(x+1) = q-1$.

To prove that $\langle x \rangle \cap \langle x+1 \rangle = \{1\}$, suppose that $x^\alpha \in \langle x+1 \rangle$ for some $\alpha$ with $0 \le \alpha < p-1$. Then $x^\alpha \equiv (x+1)^\beta$ for some $\beta$ with $\beta < q-1$. Thus $2^\beta \equiv 1 \pmod q$, so that $\beta = 0$. Thus $x^\alpha \equiv 1 \pmod{pq}$, and so $\langle x \rangle \cap \langle x+1 \rangle = \{1\}$.

The rest of the proof is as for Theorem 19. □

**Examples.** In the range $0 < n < 300$ the examples that arise from Theorem 20 are as follows, where we again include the trivial examples with $q = 3$ and therefore $x = n - 2$:

| $n$ | $p$ | $q$ | $x$ | $\xi(n)$ |
|---|---|---|---|---|
| 15 | 5 | 3 | 13 | 2 |
| 39 | 13 | 3 | 37 | 2 |
| 55 | 5 | 11 | 23 | 2 |
| 87 | 29 | 3 | 85 | 2 |
| 95 | 5 | 19 | 58 | 2 |
| 111 | 37 | 3 | 109 | 2 |
| 143 | 13 | 11 | 89 | 2 |
| 159 | 53 | 3 | 157 | 2 |
| 183 | 61 | 3 | 181 | 2 |
| 247 | 13 | 19 | 115 | 6 |
| 295 | 5 | 59 | 178 | 2 |

### 3.5. A Problem

Table 2 reveals a note-worthy phenomenon. Suppose that $m$ and $n$ are distinct integers with $\xi(n) = \xi(m) = 2$ and $|\mathbb{U}_n| = |\mathbb{U}_m|$. In many such instances we find that half of the elements of $\mathbb{U}_n$ are obtained from $\langle x \rangle_p \times \langle x+1 \rangle_q$ for some $x$ from $\mathbb{U}_n$ with $2 < x < n-2$, and that half of the elements of $\mathbb{U}_m$ are obtained from $\langle y \rangle_p \times \langle y+1 \rangle_q$ for some $y$ from $\mathbb{U}_m$ with $2 < y < n-2$. In each of these examples, we can readily see that $\mathbb{U}_m$ and $\mathbb{U}_n$ are isomorphic, but we have no explanation of why $x$ and $y$

have the same order, or of why there is no example of $x$ having order $p$ and $y$ having order $q$. Sets of composite integers exhibiting this phenomenon, with $q > 2$, are $\{55, 75\}$, $\{77, 93, 99\}$, $\{129, 147\}$, $\{143, 155, 175, 183, 225\}$ and $\{203, 215, 245, 261\}$.

## 4. Odd Composites $n$ With $\xi(n) = 4$, 6 or 12

### 4.1. Three Theorems for the Case $\xi(n) = 4$

We now give three theorems that apply to certain values of $n$ that have $\xi(n) = 4$. Theorems 21 and 22 are amplifications of Theorems 8.5 and 8.6 of Cameron and Preece [3].

**Theorem 21** *Let $n = pq$ where $p$ and $q$ are distinct primes such that $p \equiv q \equiv 5 \pmod 8$ and $\gcd(p-1,\, q-1) = 4$. If 2 is a primitive root of both $p$ and $q$, then there exist units $x$ such that*

$$\mathbb{U}_n = \langle x\rangle_4 \times \langle x+1\rangle_m = \langle x-1\rangle_m \times \langle x\rangle_4$$

*where $m = (p-1)(q-1)/4$ and $-1 \in \langle x\rangle$. There are two such $x$-values, say $x_1$ and $x_2$, with $x_1 + x_2 \equiv 0$ and $x_1x_2 \equiv 1 \pmod n$. These may be labelled so that*

$$x_1 \quad\equiv\quad \begin{cases} 2^{(p-1)/4} \pmod p \\ 2^{(q-1)/4} \pmod q \end{cases} \quad\text{and}\quad x_2 \quad\equiv\quad \begin{cases} 2^{3(p-1)/4} \pmod p \\ 2^{3(q-1)/4} \pmod q \end{cases}$$

*if $p \not\equiv q \pmod{16}$, and so that*

$$x_1 \quad\equiv\quad \begin{cases} 2^{(p-1)/4} \pmod p \\ 2^{3(q-1)/4} \pmod q \end{cases} \quad\text{and}\quad x_2 \quad\equiv\quad \begin{cases} 2^{3(p-1)/4} \pmod p \\ 2^{(q-1)/4} \pmod q \end{cases}$$

*if $p \equiv q \pmod{16}$.*

*Proof.* As $\gcd(p-1,\, q-1) = 4$, we have $\operatorname{ord}_{pq}(2) = (p-1)(q-1)/4 = m$.

The congruence $x^2 \equiv -1 \pmod n$ has four solutions, two of which are given by $x \equiv \pm x_0$ where $x_0 = 2^{m/4}$. Let the other two solutions be $x \equiv \pm x_1 \pmod n$. Then $x_1^2 \equiv -1 \pmod n$, and

$$(x_1+1)^2 = x_1^2 + 1 + 2x_1 \equiv 2x_1 \pmod n$$

so that

$$(x_1+1)^{m/2} \equiv (2x_1)^{m/4} \equiv x_0 x_1^{m/4} \pmod n\ .$$

But $x_1^2 \equiv -1 \pmod n$ and so $x_1^{m/4} \equiv \pm x_1 \pmod n$, as $m/4$ is odd. Thus

$$(x_1+1)^{m/2} \equiv \pm x_0 x_1 \pmod n\ ,$$

and so

$$(x_1 + 1)^m \equiv 1 \pmod{n} \ .$$

Let $t = \operatorname{ord}_n(x_1{+}1)$. Then $t \mid m$, and we need to show that $t = m$. As $(x_1{+}1)^t \equiv 1 \pmod{n}$ we have $(2x_1)^t \equiv 1 \pmod{n}$, whence $2^t \equiv x_1^{-t} \pmod{n}$. Thus, if $t$ were odd, $x_1$ would be a power of 2. So $t$ is even and $2^t \equiv \pm 1 \pmod{n}$. As $2^t \equiv \pm 1 \pmod{p}$, the order $t$ is a multiple of $(p-1)/2$. Similarly $t$ is a multiple of $(q-1)/2$, and so $t = m$ or $m/2$. But

$$(x_1 + 1)^{m/2} \equiv \pm x_0 x_1 \not\equiv 1 \pmod{n} \ .$$

So $t = m$, as required.

We now prove that $\langle x_1 \rangle \cap \langle x_1{+}1 \rangle = \{1\}$. If $\pm x_1 \in \langle x_1{+}1 \rangle$ then $-1 = x_1^2 \in \langle x_1{+}1 \rangle$. So suppose $-1 \in \langle x_1 + 1 \rangle$. This requires $(x_1 + 1)^{m/2} \equiv -1 \pmod{n}$, *i.e.* $x_0 x_1 \equiv \pm 1 \pmod{n}$, which is false.

Thus $\mathbb{U}_n = \langle x \rangle \times \langle x + 1 \rangle$. The two values of $x$ are $x_1$ and $x_2 \equiv -x_1$; for them, $x_1 + x_2 \equiv 0$ and $x_1 x_2 \equiv -x_1^2 \equiv +1 \pmod{n}$.

The argument for $\langle x - 1 \rangle$ is similar.

If $x^2 \equiv -1 \pmod{n}$, then $x \equiv 2^{(p-1)/4}$ or $2^{3(p-1)/4} \pmod{p}$ and $x \equiv 2^{(q-1)/4}$ or $2^{3(q-1)/4} \pmod{q}$. The combinations excluded in the statement of the Theorem are precisely those that give $x = \pm x_0$. For example, if $p \equiv 5 \pmod{16}$ and $q \equiv 13 \pmod{16}$, say $p = 16u + 5$ and $q = 16v + 13$, then

$$\begin{aligned} x_0 &\equiv 2^{((p-1)/4)((q-1)/4)} \\ &\equiv 2^{((p-1)/4)(4v+3)} \\ &\equiv 2^{3(p-1)/4} \pmod{p} \end{aligned}$$

and

$$\begin{aligned} x_0 &\equiv 2^{((q-1)/4)(4u+1)} \\ &\equiv 2^{(q-1)/4} \pmod{q} \ . \end{aligned}$$

□

**Note.** In the range $0 < n < 300$, Theorem 21 covers these parameter sets:

| $n$ | $p, q$ | $x_1, x_2$ | $p \equiv q \pmod{16}$ ? |
|---|---|---|---|
| 65 | $5, 13$ | $47, 18$ | No |
| 145 | $5, 29$ | $12, 133$ | No |
| 185 | $5, 37$ | $117, 68$ | Yes |
| 265 | $5, 53$ | $182, 83$ | Yes |

**Theorem 22** *Let $n = pq$, where $p$ and $q$ are primes such that $p \equiv 5 \pmod{8}$, $q \equiv 1 \pmod{16}$, and $\gcd(p-1, q-1) = 4$. If 2 is a primitive root of $p$ and*

$\mathrm{ord}_q(2) = (q-1)/2$, *then there exist units $x$ such that*

$$\mathbb{U}_n = \langle x\rangle_4 \times \langle x+1\rangle_m = \langle x-1\rangle_m \times \langle x\rangle_4$$

*where $m = (p-1)(q-1)/4$ and $-1 \in \langle x\rangle$. There are four such $x$-values, say $x_1$, $x_2$, $x_3$ and $x_4$, with $x_1 + x_2 \equiv x_3 + x_4 \equiv 0$ and $x_1x_2 \equiv x_3x_4 \equiv 1 \pmod n$. These may be labelled so that*

$$x_1 \equiv \begin{cases} 2^{(p-1)/4} \pmod p \\ 2^{(q-1)/8} \pmod q \end{cases} \quad \text{and} \quad x_2 \equiv \begin{cases} 2^{3(p-1)/4} \pmod p \\ 2^{3(q-1)/8} \pmod q \end{cases}$$

*and*

$$x_3 \equiv \begin{cases} 2^{(p-1)/4} \pmod p \\ 2^{3(q-1)/8} \pmod q \end{cases} \quad \text{and} \quad x_4 \equiv \begin{cases} 2^{3(p-1)/4} \pmod p \\ 2^{(q-1)/8} \pmod q \end{cases} .$$

*Proof.* As $\gcd(p-1, (q-1)/2) = 4$, we have $\mathrm{ord}_{pq}(2) = (p-1)(q-1)/8 = m/2$. The congruence $x^2 \equiv -1 \pmod n$ has four solutions, say $\pm x_1$ and $\pm x_3$. By Lemma 1.4 of [1], none of these solutions is a power of 2. Let $x$ be any one of these four values, and write $s = m/2$. Then $\mathrm{ord}_n(x) = 4$ and $(x+1)^2 \equiv 2x \pmod n$. Thus $(x+1)^m \equiv 2^s x^s \equiv x^s \pmod n$ where $s$ is a multiple of 4. So $(x+1)^m \equiv 1 \pmod n$.

Let $t = \mathrm{ord}_n(2x)$. Then $t \mid s$ and $2^t \equiv x^{-t} \pmod n$. But $x$ is not a power of 2, so $t$ is even and $2^t \equiv \pm 1 \pmod n$. Thus $t$ is a multiple of both $(p-1)/2$ and $(q-1)/4$, and so is a multiple of $(p-1)(q-1)/16 = s/2$. So $t = s/2$ or $s$, whence $\mathrm{ord}_n(x+1) = m/4$ or $m/2$ or $m$. However, $(x+1)^{m/2} \equiv (2x)^{m/4} \equiv 2^{m/4} \not\equiv 1 \pmod n$, so $\mathrm{ord}_n(x+1) = m$.

To establish that $\langle x\rangle \cap \langle x+1\rangle = \{1\}$, suppose that $-1 \in \langle x+1\rangle$. Then $(x+1)^s \equiv -1$, whence $(2x)^{m/4} \equiv (x+1)^s \equiv -1 \pmod n$, so that $2^{m/4} \equiv -1 \pmod n$, again contradicting Lemma 1.4 of [1]. Thus $\langle x\rangle \cap \langle x+1\rangle = \{1\}$.

The argument for $\langle x-1\rangle$ is similar.

If $x^2 \equiv -1$, then $x \equiv 2^{(p-1)/4}$ or $2^{3(p-1)/4} \pmod p$ and $x \equiv 2^{(q-1)/8}$ or $2^{3(q-1)/8} \pmod q$. The four values of $x$ come from the four possible combinations. □

**Note.** In the range $0 < n < 300$, Theorem 22 covers these parameter sets:

| $n$ | $p$ | $q$ | $x_1, x_2$ | $x_3, x_4$ |
|---|---|---|---|---|
| 85 | 5 | 17 | $72, 13$ | $47, 38$ |
| 221 | 13 | 17 | $21, 200$ | $47, 174$ |

**Theorem 23** *Let $n = pq$ where $p$ and $q$ are primes such that $p \equiv 5 \pmod 8$, $q \equiv 9 \pmod{16}$ and $\gcd(p-1, q-1) = 4$. Suppose that 2 is a primitive root of $p$ and that $\mathrm{ord}_q(2) = (q-1)/2$. Then there exist units $x$ such that half of the elements in $\mathbb{U}_n$ are provided by $\langle x\rangle_4 \times \langle x+1\rangle_{m/2} = \langle x-1\rangle_{m/2} \times \langle x\rangle_4$, where $m = (p-1)(q-1)/4$ and $-1 \in \langle x\rangle$. There are two such $x$-values, say $x_1$ and $x_2$, with $x_1 + x_2 \equiv 0$ and $x_1x_2 \equiv 1 \pmod n$. These may be labelled so that*

$$x_1 \equiv \begin{cases} 2^{(p-1)/4} \pmod{p} \\ 2^{(q-1)/8} \pmod{q} \end{cases} \quad \text{and} \quad x_2 \equiv \begin{cases} 2^{3(p-1)/4} \pmod{p} \\ 2^{3(q-1)/8} \pmod{q} \end{cases}$$

*if* $2p \equiv q + 17 \pmod{32}$*; and so that*

$$x_1 \equiv \begin{cases} 2^{(p-1)/4} \pmod{p} \\ 2^{3(q-1)/8} \pmod{q} \end{cases} \quad \text{and} \quad x_2 \equiv \begin{cases} 2^{3(p-1)/4} \pmod{p} \\ 2^{(q-1)/8} \pmod{q} \end{cases}$$

*if* $2p \equiv q + 1 \pmod{32}$.

*Proof.* The proof parallels that of Theorem 21. Here, $x_0 = 2^{m/8}$. As there, the posssibilities are obtained by excluding the combinations that give $x = \pm x_0$. □

**Note.** In the range $0 < n < 300$, Theorem 23 covers the following parameter set, which has $2p \equiv q + 1 \pmod{32}$:

| $n$ | $p$ | $q$ | $x_1, x_2$ |
|---|---|---|---|
| 205 | 5 | 41 | 132, 73 |

The case $2p \equiv q + 17 \pmod{32}$ arises when we take $(n, p, q, x_1) = (533, 13, 41, 73)$.

### 4.2. A Problem

For some of the values $n$ covered by Theorem 21, we find that $\mathbb{U}_n$ is given by a decomposition of the form $\langle x \rangle_{x+1} \times \langle x+1 \rangle_b$, perhaps even with $x(x+1) \equiv 2 \pmod{n}$, but not necessarily with $b = 4$. We have no explanation for this. Some details are as follows:

| $n$ | $p, q$ | $\mathbb{U}_n$ | $x(x+1) \equiv 2$ ? |
|---|---|---|---|
| 65 | 5, 13 | $\langle 11 \rangle_{12} \times \langle 12 \rangle_4$ | Yes |
| 145 | 5, 29 | $\langle 27 \rangle_{28} \times \langle 28 \rangle_4$ | No |
| 185 | 5, 37 | – | – |
| 265 | 5, 53 | $\langle 51 \rangle_{52} \times \langle 52 \rangle_4$ | Yes |
| 305 | 5, 61 | – | – |
| 377 | 13, 29 | $\langle 27 \rangle_{28} \times \langle 28 \rangle_{12}$ | Yes |

### 4.3. Three Thorems for the Case $\xi(n) = 6$

We now give three theorems that apply to certain values of $n$ with $\xi(n) = 6$. Our Theorem 24 is an amplification of Theorem 8.7 of the revised version of Cameron and Preece [3].

**Theorem 24** *Let* $n = pq$*, with* $\xi(n) = 6$*, where* $p$ *and* $q$ *are primes with* $p \equiv q \equiv 7 \pmod{12}$*. Assume that* 3 *is a negating primitive* $\lambda$*-root of* $n$*. (This holds, in* *particular, if* $3$ *is a primitive root of both* $p$ *and* $q$*.) Assume further that there exists a unit* $x$ *satisfying* $x^2 \equiv x - 1 \pmod{n}$ *such that* $x \notin \langle 3 \rangle$ *and* $-1 \notin \langle x+1 \rangle$*, and such that* $x + 1$ *has even order. Then*

$$\mathbb{U}_n = \langle x \rangle_6 \times \langle x+1 \rangle_\mu$$

*where* $\mu = (p-1)(q-1)/6$*. Also, half of the elements in* $\mathbb{U}_n$ *are provided by*

$$\langle\ -(x+1)\ \rangle_\mu \times \langle\ -x\ \rangle_3\ ,$$

*and no two elements in this set are the negatives of one another. If such a value of* $x$ *exists, then its inverse could be used in its place, so there are two such values, say* $x_1$ *and* $x_2$*, with* $x_1 + x_2 \equiv x_1 x_2 \equiv 1 \pmod{n}$*. These may be described as follows:*

$$x_1 \quad \equiv \quad \begin{cases} s_p \pmod{p} \\ s_q \pmod{q} \end{cases} \quad \text{and} \quad x_2 \quad \equiv \quad \begin{cases} s_p^5 \pmod{p} \\ s_q^5 \pmod{q} \end{cases},$$

*where* $s_p$ *and* $s_q$ *are elements of order* $6$ *in* $\mathbb{Z}_p$ *and* $\mathbb{Z}_q$ *respectively.*

*Proof.* We have $3^\mu \equiv 1$ and $3^{\mu/2} \equiv -1 \pmod{n}$. Thus $3^{\mu/6}$ is an element of order 6 whose cube is $-1$ and which is not $x$ or $x^{-1}$.

At least two solutions of $x^2 \equiv x - 1 \pmod{n}$ will satisfy $x \notin \langle 3 \rangle$. Consider any $x$ satisfying the conditions of the theorem. Then, as $\mu/2$ is an odd multiple of 3, we have $3^{\mu/2} \equiv -1 \equiv x^{\mu/2}$, so $(3x)^{\mu/2} \equiv 1 \pmod{n}$. If $(3x)^{\mu/6} \equiv 1$ then $3^{\mu/6}x^{\mu/6} \equiv 1$ which, since $\mu/6$ is odd, implies that $3^{\mu/6}x \equiv 1$ or $3^{\mu/6} \equiv -1$ or $3^{\mu/6} \equiv x$. None of these is possible; thus $(3x)^{\mu/6} \not\equiv 1 \pmod{n}$.

Let $\beta = \mathrm{ord}_n(3x)$, and write $\mu/2 = 3\alpha$ where $\alpha$ is odd. Then $(3x)^\beta \equiv 1$ and $\beta \mid 3\alpha$, but $\beta \nmid \alpha$. So $\beta = 3\zeta$ where $\zeta \mid \alpha$. Then $(3x)^{3\zeta} \equiv 1$ and $x^{3\zeta} \equiv -1$, so $3^{3\zeta} \equiv -1$. Thus $3^{6\zeta} \equiv 1$ and $6\alpha \mid 6\zeta$, *i.e.* $\alpha \mid \zeta$. But $\zeta \mid \alpha$, so $\alpha = \zeta$ and $\beta = \mu/2$. Thus $\mathrm{ord}_n(3x) = \mu/2$.

Write $\mathrm{ord}_n(1+x) = 2k$, as the order is even. Then $(3x)^k \equiv (1+x)^{2k} \equiv 1$, so $k = \mu/2$ as $2k \le \mu$. Thus $\mathrm{ord}_n(1+x) = \mu$.

We now show that, for this $x$, we have $\langle x \rangle \cap \langle x+1 \rangle = \{1\}$. (All congruences are modulo $n$.) As $-1 \notin \langle x+1 \rangle$ we have $x \notin \langle x+1 \rangle$. Suppose that $-x \in \langle x+1 \rangle$; then $-x \equiv (x+1)^\epsilon$ for some $\epsilon$, and $1 \equiv (x+1)^{3\epsilon}$ so that $\mu \mid 3\epsilon$. Thus $\epsilon$ is even, say $\epsilon = 2\theta$. Then $(x+1)^{6\theta} \equiv 1$, so $\mu \mid 6\theta$, *i.e.* $\alpha \mid \theta$. Thus $2\alpha \mid \epsilon$, so $\epsilon = 2\alpha$ or $4\alpha$, whence $-x \equiv (x+1)^{\mu/3}$ or $(x+1)^{2\mu/3}$. So $(x+1)^{\mu/3} \equiv -x$ or $x^2$. But if $-x \equiv (x+1)^{\mu/3}$ then $-x \equiv (3x)^{\mu/6}$, which is congruent to $3^{\mu/6}x$ or $-3^{\mu/6}$ or $-x^2 3^{\mu/6}$, whence $3^{\mu/6} \equiv -1$ or $x \equiv 3^{\mu/6}$ or $x \equiv 3^{-\mu/6}$, all of which are impossible. So $-x \not\equiv (x+1)^{\mu/3}$. Similarly $x^2 \not\equiv (x+1)^{\mu/3}$, so $-x \notin \langle x+1 \rangle$, Thus $\langle x \rangle \cap \langle x+1 \rangle = \{1\}$.

We next show that $\mathrm{ord}_n(1+x^{-1})$ is also even. Let this order be $h$, so that $(1+x^{-1})^h \equiv 1$, whence $(1+x)^h \equiv x^h$. But $\langle x \rangle \cap \langle 1+x \rangle = \{1\}$, so $x^h \equiv 1$. Thus $6 \mid h$, whence $h$ is even. Thus $x^{-1}$ can indeed be used instead of $x$ provided that $-1 \notin \langle x^{-1}+1 \rangle$. Suppose on the contrary that $-1 \equiv (x^{-1}+1)^\ell$. Then

$(x+1)^\ell \equiv -x^\ell \equiv x^{\ell+3}$. Hence $x^{\ell+3} \equiv 1$ and $(x+1)^\ell \equiv 1$. The first of these conditions requires that $\ell \equiv 3 \pmod{6}$, whereas the second requires that $\ell$ is even. So $-1 \notin \langle x^{-1}+1\rangle$. Finally, the proof that $\langle x^{-1}+1\rangle \cap \langle x^{-1}\rangle = \{1\}$ is straightforward.

The proofs of the assertions about $\langle -(x+1)\rangle_\mu \times \langle -x\rangle_3$ are similar to the proof above. □

**Corollary 25** *Let $n = 7q$ where $q$ is a prime, $q \equiv 7 \pmod{12}$, that has 3 as a primitive root. Suppose that $\xi(n) = 6$, and that there exists a unit $x$ such that $x^2 \equiv x-1 \pmod{n}$, $x \notin \langle 3\rangle$, and $-1 \notin \langle x+1\rangle$. Then there are two values $x_1$ and $x_2$ of $x$ such that $x_1 + x_2 \equiv x_1x_2 \equiv 1 \pmod{n}$ and $x_1 \equiv 3 \pmod{7}$. Further, if, for $i = 1, 2$, the unit $z_i$ is defined by $z_i \equiv 4 \pmod{7}$ and $z_i \equiv x_i \pmod{q}$, so that $z_1 + z_2 \equiv 1 \pmod{n}$, then $z_1$ and $z_2$ are two values of $z$ for which $\mathbb{U}_n = \langle z\rangle_6 \times \langle z+1\rangle_{q-1}$.*

*Proof.* The only solutions of $x_1x_2 \equiv x_1 + x_2 \equiv 1 \pmod{7}$ are given by $\{x_1, x_2\} = \{3, 5\}$. Let $q = 6v + 1$ where $v$ is odd. Then in the usual notation $\mu = q - 1 = 6v$. We note that $\mathrm{ord}_n(z_1) = \mathrm{lcm}(\mathrm{ord}_7(4), \mathrm{ord}_q(x_1)) = \mathrm{lcm}(3, 6) = 6$. Consider first the case when $\mathrm{ord}_n(x_1 + 1)$ is even. Then, as in the proof of Theorem 24, we have $\mathrm{ord}_n(x_1 + 1) = \mu$. Thus

$$6v = \mathrm{ord}_n(x_1 + 1) = \mathrm{lcm}(\mathrm{ord}_7(x_1 + 1), \mathrm{ord}_q(x_1 + 1)) = \mathrm{lcm}(3, \mathrm{ord}_q(x_1 + 1)) ,$$

so that $\mathrm{ord}_q(x_1 + 1)$ is even and hence

$$\mathrm{ord}_n(z_1 + 1) = \mathrm{lcm}(6, \mathrm{ord}_q(x_1 + 1)) = \mathrm{lcm}(3, \mathrm{ord}_q(x_1 + 1)) = \mu .$$

Consider next the case when $\mathrm{ord}_n(x_1 + 1)$ is odd, say $\mathrm{ord}_n(x_1 + 1) = h$. Then $\mathrm{ord}_n((x_1 + 1)^2) = h$ so that $\mathrm{ord}_n(3x) = h$. But, as in the proof of Theorem 24, $\mathrm{ord}_n(3x) = \mu/2 = 3v$; so $3v = \mathrm{ord}_n(x_1 + 1) = \mathrm{lcm}(3, \mathrm{ord}_q(x_1 + 1))$ and hence $\mathrm{ord}_n(z_1 + 1) = \mathrm{lcm}(6, \mathrm{ord}_q(x_1 + 1)) = 6v = \mu$. Thus in each case $\mathrm{ord}_n(z_1 + 1) = \mu$.

We must now show that $\langle z_1\rangle \cap \langle z_1 + 1\rangle = \{1\}$. To do this it suffices to show that neither $z_1^2$ nor $z_1^3$ is in $\langle z_1 + 1\rangle$. Suppose first that $z_1^3 = (z_1 + 1)^\alpha$ where $0 < \alpha < 6v$. Then $4^3 = 5^\alpha \pmod{7}$, whence $6 \mid \alpha$ so that $\alpha$ is even. But $1 \equiv z_1^6 \equiv (z_1+1)^{2\alpha}$ so that $6v \mid 2\alpha$, *i.e.* $3v \mid \alpha$. Thus $6v \mid \alpha$, a contradiction. Suppose now that $z_1^2 \equiv (z_1 + 1)^\beta$ where $0 < \beta < 6v$. Then $1 \equiv (z_1 + 1)^{3\beta}$ so that $6v \mid 3\beta$, *i.e.* $2v \mid \beta$. Thus $\beta = 2v$ or $4v$. First consider the possibility $\beta = 2v$. Then $z_1^2 \equiv (z_1 + 1)^{2v} \pmod{n}$. Thus $4^2 \equiv 5^{2v} \pmod{7}$, so $4^v \equiv 2 \pmod{7}$, so that $v \equiv 2 \pmod{3}$. But $v$ is odd, so $v \equiv 5 \pmod{6}$ and $v - 2$ is an odd multiple of 3. Further, $x_1^2 \equiv (x_1 + 1)^{2v} \pmod{q}$, so that $x_1^2 \equiv (3x_1)^v \pmod{q}$, whence $x_1^{v-2} \equiv 3^{-v} \pmod{q}$. As $v - 2$ is an odd multiple of 3, we have $x_1^{v-2} \equiv -1 \pmod{q}$, so $3^v \equiv -1 \pmod{q}$ and $3^{2v} \equiv 1 \pmod{q}$, contradicting the requirement for 3 to be a primitive root of $q$. The second possibility is dealt with similarly.

Finally, the proofs for $z_2$ are almost identical to those for $z_1$. Now we have $\mathrm{ord}_n(z_2 + 1) = \mathrm{lcm}(6,\ 3v \text{ or } 6v) = 6v$. □

**Notes.** It is easily shown that if $\mathrm{ord}_n(x_1+1)=\mu$ then $(z_1+1)^{\mu/2}\equiv -1 \pmod{n}$, so that $z_1+1$ is negating.

As confusion has arisen over the cases covered by Theorem 24, and the conditions of the theorem and its corollary are intricate, we provide Table 4 to give more details of the coverage than was given for previous situations.

**Theorem 26** *Let $n=pq$, with $\xi(n)=6$, where $p$ and $q$ are primes with $p\equiv 7 \pmod{12}$ and $q\equiv 1 \pmod{12}$. Assume that 3 is non-negating in $\mathbb{U}_n$ and that $\mathrm{ord}_n(3)=\mu/2$ where $\mu=(p-1)(q-1)/6$. Then there exist units $x$, satisfying $x^2\equiv x-1$, such that*

$$\mathbb{U}_n=\langle x\rangle_6\times\langle x+1\rangle_\mu$$

*and*

$$\mathbb{U}_n=V_n\cup(-V_n)$$

*where $V_n=\langle -(x+1)\rangle_\mu\times\langle -x\rangle_3$. Such $x$-values exist in pairs $(x_1,x_2)$ with $x_1+x_2\equiv x_1x_2\equiv 1 \pmod{n}$. There is one such pair, except that two pairs arise precisely when $3^{\mu/6}\equiv 1$ (mod $p$ or mod $q$).*

*Proof.* No $x$ satisfying $x^2\equiv x-1 \pmod{n}$ can be a power of 3, as otherwise we would have $-1\equiv x^3\in\langle 3\rangle$.

As $6\mid \mu/2$, we have $(3x)^{\mu/2}=3^{\mu/2}x^{\mu/2}\equiv 1 \pmod{n}$. Thus, as $(x+1)^2\equiv 3x$, we have $(1+x)^\mu\equiv 1 \pmod{n}$.

Suppose that $\mathrm{ord}_n(x+1)$ is odd. Then $\mathrm{ord}_n((x+1)^2)$ is also odd and so, since $(x+1)^2\equiv 3x$, we have $(sx)^h\equiv 1 \pmod{n}$ for some odd integer $h$. Consideration of the three cases $h\equiv 1$, 3 or 5 (mod 6) yields $3^{-h}\equiv -x$, 1 or $-x$ (mod $n$), none of which is possible. So $\mathrm{ord}_n(x+1)$ must be even.

Let $\mathrm{ord}_n(x+1)=2k$. Then $\mathrm{ord}_n(3x)=k$ where $k\mid\mu/2$. We consider the relation $(3x)^k\equiv 1 \pmod{n}$ in six separate cases, according as $k\equiv\ell \pmod{6}$, $\ell=0,1,\ldots,5$.

(a) $\ell=0$: Here $x^k\equiv 1$, so $3^k\equiv 1$ and so $k=\mu/2$.
(b) $\ell=1$: Here $3^k\equiv x^{-1}$, so $3^{3k}\equiv -1$, which contradicts "3 is non-negating".
(c) $\ell=2$: Here $3^k\equiv -x$, so $3^{3k}\equiv 1$, and so $\mu/2\mid 3k$, whence $k=\mu/6$ or $\mu/2$.
(d) $\ell=3$: Here we have $3^k\equiv -1$, which is impossible.
(e) $\ell=4$: Here $3^k\equiv x^2$ and $3^{3k}\equiv 1$, giving $k=\mu/6$ or $\mu/2$.
(f) $\ell=5$: Here we have $3^k\equiv x$, which is impossible.

So consider the possibility that $k=\mu/6$. Then $(3x)^{\mu/6}\equiv 1$ so $3^{\mu/6}x^{\mu/6}\equiv 1$. However, as $\mu/6$ is even we have $x^{\mu/6}\equiv x^2$ or $-x$. So $3^{\mu/6}\equiv -x$ or $x^2$ and so $x\equiv -3^{\mu/6}$ or $-3^{\mu/3}$.

However, $x\equiv -3^{\mu/6}$ if and only if $x^{-1}\equiv -3^{\mu/3}$. So we obtain only one pair of values of $x$ precisely when $x\equiv -3^{\mu/6}$ is a solution of $x^2\equiv x-1$, *i.e.* when $x\equiv 3^{\mu/6}$ is a solution of $x^2\equiv -x-1 \pmod{n}$. So we obtain two pairs of values of $x$ precisely when $x\equiv 3^{\mu/6}$ is not a solution of both $x^2+x+1\equiv 0 \pmod{p}$ and $x^2+x+1\equiv 0 \pmod{q}$. But $x\equiv 3^{\mu/6}$ is a solution of $x^3-1\equiv(x-1)(x^2+x+1)\equiv 0$ (mod $p$

and mod $q$); so we have two pairs of values of $x$ precisely when $3^{\mu/6} \equiv 1 \pmod{p \text{ or } \bmod q}$.

For these values of $x$ we have $\mathrm{ord}_n(x+1) = \mu$. We now show that $-1 \notin \langle x+1 \rangle$. Suppose the contrary; then we must have $-1 \equiv (x+1)^{\mu/2}$, so that $(3x)^{\mu/4} \equiv -1$. But $\mu/4$ is an odd multiple of 3, so $-1 \equiv (3x)^{\mu/4} \equiv -3^{\mu/4}$, contradicting the assumption that $\mathrm{ord}_n(3) = \mu/2$. The proof that $\langle x \rangle \cap \langle x+1 \rangle = \{1\}$ now follows as for Theorem 24. □

**Note.** In the range $0 < n < 2000$, Theorem 26 covers parameter sets as follows:

| $n$ | $p$ | $q$ | $x_1$,$x_2$ | |
|---|---|---|---|---|
| 91 | 7 | 13 | 75,17 | |
| 247 | 19 | 13 | 179,69 | 160,88 |
| 403 | 31 | 13 | 88,316 | |
| 511* | 7 | 73 | ‡ | |
| 559 | 43 | 13 | 179,381 | |
| 679 | 7 | 97 | 327,353 | |
| 763 | 7 | 109 | 264,500 | 591,173 |
| 871 | 67† | 13 | 842,30 | 231,641 |

| $n$ | $p$ | $q$ | $x_1$,$x_2$ | |
|---|---|---|---|---|
| 1027 | 79 | 13 | 530,498 | |
| 1267 | 7 | 181 | 411,857 | 773,495 |
| 1339 | 103† | 13 | 1180,160 | 881,459 |
| 1351** | 7 | 193 | ‡ | |
| 1603 | 7 | 229 | 782,822 | |
| 1651 | 127 | 13 | 1505,147 | 108,1544 |
| 1687 | 7 | 241 | 467,1221 | |
| 1807 | 139 | 13 | 1070,738 | |
| 1843 | 19 | 97 | 1323,521 | 715,1129 |
| 1939 | 7 | 277 | 948,992 | |
| 1963 | 151 | 13 | 270,1694 | 335,1629 |

* $\mathrm{ord}_n(3) = \mu/6$
** $\mathrm{ord}_n(3) = \mu/4$
† $\mathrm{ord}_p(3) = (p-1)/3$
‡ fails as $\mathrm{ord}_n(3) \neq \mu/2$

**Theorem 27** *Let $n = pq$, with $\xi(n) = 6$, where $p$ and $q$ are primes with $p \equiv 7 \pmod{12}$ and $q \equiv 13 \pmod{24}$. Assume that 3 is negating in $\mathbb{U}_n$ and that $\mathrm{ord}_n(3) = \mu/2$ where $\mu = (p-1)(q-1)/6$. Assume further that there exists a unit $x$ satisfying $x^2 \equiv x - 1 \pmod{n}$ such that $x \notin \langle 3 \rangle$ and $-1 \notin \langle x+1 \rangle$, and such that $x+1$ has even order. Then*

$$\langle x \rangle_6 \times \langle x+1 \rangle_{\mu/2}$$

*gives half of the elements of $\mathbb{U}_n$. If such a value of $x$ exists then its inverse could be used in its place, so there are two such values, say $x_1$ and $x_2$, with $x_1 + x_2 \equiv x_1 x_2 \equiv 1 \pmod{n}$.*

*Proof.* We have $\mathrm{ord}_n(3) = \mu/2$ and $3^{\mu/4} \equiv -1 \pmod{n}$. So, as $\mu/4$ is an odd multiple of 3, we have $(3x)^{\mu/4} \equiv 3^{\mu/4} x^{\mu/4} \equiv (-1)(-1) \equiv 1 \pmod{n}$. Thus, as $(x+1)^2 \equiv 3x$, we have $(x+1)^{\mu/2} \equiv 1 \pmod{n}$.

Let $\mathrm{ord}_n(x+1) = 2k$ for some $k$. Then $\mathrm{ord}_n(3x) = k$ and $k \mid \mu/4$. We consider the relationship $(3x)^k \equiv 1 \pmod{n}$ for the three possible cases $k = 1, 3$ or $5 \pmod{6}$.

(a) If $k \equiv 1 \pmod 6$ then $x^k \equiv x$ so $x \equiv 3^{-k}$, which contradicts the assumption that $x \notin \langle 3 \rangle$.

(b) If $k \equiv 3 \pmod 6$ then $x^k \equiv -1 \pmod n$, so $3^k \equiv -1$. Thus $k$ is an odd multiple of $\mu/4$, whence $k = \mu/4$.

(c) If $k \equiv 5 \pmod 6$ then $x^k \equiv x^{-1}$, whence $3^k \equiv x$, which is impossible.

We therefore conclude that $k \equiv \mu/4$ and $\text{ord}_n(x+1) = \mu/2$. The rest of the proof is similar to that of Theorem 24. □

**Corollary 28** *Suppose that the conditions of Theorem 27 are met, with $p = 7$. Then the values $x_i$ can be labelled so that $x_1 \equiv 3 \pmod 7$, and, if, for $i = 1, 2$, we have $z_i \equiv 4 \pmod 7$ and $z_i \equiv x_i \pmod q$, then $\langle z_i \rangle_6 \times \langle z_i + 1 \rangle_{(q-1)/2}$ provides half of the units if $\mathbb{U}_n$.*

*Proof.* Similar to the proof of Corollary 25. □

**Note.** In the range $0 < n < 2000$, Theorem 27 and Corollary 28 give us these parameter sets:

| $n$ | $p$ | $q$ | $x_1$,$x_2$ | $z_1$,$z_2$ |
|---|---|---|---|---|
| 259 | 7 | 37 | 101,159 | 249,11 |
| 427 | 7 | 61 | 353,75 | 109,319 |
| 1099 | 7 | 157 | ‡ | 641,459 |
| 1159 | 19 | 61 | 563,597 | — |
| 1591 | 43 | 37 | 566,1026 | — |

‡ fails as $\text{ord}(x_1 + 1)$ is odd

**Note.** $\mathbb{U}_{259} = \langle 177 \rangle_{12} \times \langle 178 \rangle_{18} = \langle 178 \rangle_{18} \times \langle 179 \rangle_{12}$. This is not covered by any simple general result, as $177 \equiv 178^6 \times 179^5 \pmod{259}$.

### 4.4. An Extension for $\xi(n) = 12$

**Theorem 29** *Let $n = pq$, with $\xi(n) = 12$, where $p$ and $q$ are primes, $p \equiv q \equiv 1 \pmod{12}$. Assume that 3 is non-negating in $\mathbb{U}_n$ and that $\text{ord}_n(3) = \mu/2$ where $\mu = (p-1)(q-1)/12$. Then there exist units $x$ satisfying $x^2 \equiv x - 1 \pmod n$ such that $\langle x \rangle_6 \times \langle x+1 \rangle_\mu$ gives half of the elements of $\mathbb{U}_n$. Such values exist in pairs $(x_1, x_2)$ with $x_1 + x_2 = x_1 x_2 \equiv 1 \pmod n$. There is one such pair, except that two pairs occur precisely when $3^{\mu/6} \equiv 1$ (mod $p$ or mod $q$).*

*Proof.* As for Theorem 26. □

**Note.** In the range $0 < n < 2000$, Theorem 29 covers these parameter sets:

| $n$ | $p$ | $q$ | $x_1$,$x_2$ | |
|---|---|---|---|---|
| 481 | 13 | 37 | 101,381 | 270,212 |
| 793 | 13 | 61 | 719,75 | 563,231 |
| 1261 | 13 | 97 | $62, 1200$ | |

## 5. Some More Lifts

Inspection of Tables 2 and 3 reveals many more examples of decompositions that can be viewed as lifts, when that concept is generalised in the obvious way from how it was given in Section 2.3. We have particular need of lifts from $n = pq$, where $p$ and $q$ are distinct odd primes, to $n = pq^2$.

Consider, for example, the decomposition $\mathbb{U}_{15} = \langle 13\rangle_4 \times \langle 14\rangle_2$. Here the orders of the generators are given by $\text{ord}_{15}(13) = 4$ and $\text{ord}_{15}(14) = 2$. Now, with a view to lifting from $n = 15$ to $n = 45$, consider the values

$$\text{ord}_{45}(13 + 15i) \quad = \quad \begin{cases} 12, & i = 0,\, 2 \\ \ 4, & i = 1 \end{cases}$$

and

$$\text{ord}_{45}(14 + 15j) \quad = \quad \begin{cases} 6, & j = 0,\, 1 \\ 2, & j = 2 \end{cases} \quad .$$

It follows that we have the lifts given by $\mathbb{U}_{45} = \langle 43\rangle_{12} \times \langle 44\rangle_2 = \langle 28\rangle_4 \times \langle 29\rangle_6$. Likewise we have the lifts given by $\mathbb{U}_{75} = \langle 73\rangle_{20} \times \langle 74\rangle_2 = \langle 43\rangle_4 \times \langle 44\rangle_{10}$.

## 6. Odd Composite Integers $n$ With $\xi(n) > 6$

In the range $0 < n < 300$ there are 4 composite odd values of $n$ with $\xi(n) > 6$, namely 195, 255, 273 and 275. We now give a theorem that covers the last of these, the other values being covered in Section 7 below, this theorem employing a lift from $5p$ to $5^2p$.

**Theorem 30** *Let $n = 25p$ where $p$ is a prime, $p \equiv 11 \pmod{20}$, having 2 as a primitive root. Then precisely half of the elements of $\mathbb{U}_n$ are provided by*

$$\langle x\rangle_5 \times \langle x + 1\rangle_{2(p-1)}$$

*for each of the values $x = 5p + 1$, $10p + 1$, $15p + 1$ and $20p + 1$.*

*Proof.* A straightforward argument shows that $\text{ord}_{25p}(x) = 5$ for each $x$, so now consider $x + 1 = 5pm + 2$. As $x + 1 \equiv 2 \pmod{p}$ and 2 is a primitive root of $p$, we have $\mathrm{ord}_p(x+1) = p-1$. Thus, as $\mathrm{ord}_{25}(x+1) = 20$, we have $\mathrm{ord}_{25p}(x+1) = \mathrm{lcm}(p-1,\, 20) = 2(p-1)$.

Suppose that $x^a \in \langle x+1 \rangle$ for some $a$ with $0 \le a \le 4$. Then $x^a \equiv (x+1)^b \pmod{25p}$ for some $b$ with $0 \le b \le 2p-3$. Then $2^b \equiv 1 \pmod{p}$, so $b = 0$ or $p-1$. But also $2^b \equiv 1 \pmod{5}$, so $b$ is a multiple of 4. Thus $b = 0$ and $x^a = 1$. Thus $\langle x \rangle \cap \langle x+1 \rangle = \{1\}$. □

**Note.** For $n = 275 = 25 \times 11$, half of the elements of $\mathbb{U}_n$ are provided by $\langle x \rangle_5 \times \langle x+1 \rangle_{20}$ with $x$ taking any of the values 56, 111, 166 and 221.

## 7. Odd Composite Integers $n = 3pq$

We now provide two theorems which, in the range $0 < n < 300$, cover certain $n$-values with $\xi(n) = 4$, 8 or 12. These theorems involve lifts from $pq$ to $3pq$, where $p$ and $q$ are distinct primes greater than 3.

**Theorem 31** *Let $n = 3pq$ where $p$ and $q$ are distinct primes greater than 3. Let $x$ be any integer, $1 < x < pq-1$, such that $\mathbb{U}_{pq} = \langle x \rangle_a \times \langle x+1 \rangle_b \pmod{pq}$ for some $a$ and $b$, each greater than 1, with $b$ even. Let $k$ be the value, taken from $\{0,1,2\}$, such that $x + kpq \equiv 1 \pmod{3}$. Then precisely half of the members of $\mathbb{U}_n$ are contained in*

$$\langle x + kpq \rangle_a \times \langle x + kpq + 1 \rangle_b \ .$$

*Proof.* We have $\mathrm{ord}_{pq}(x) = a$ and $\mathrm{ord}_{pq}(x+1) = b$, where $ab = (p-1)(q-1)$. Also $\langle x \rangle \cap \langle x+1 \rangle = \{1\}$ in $\mathbb{Z}_{pq}$.

Choose $k$ from $\{0,1,2\}$ so that $y = x + kpq \equiv 1 \pmod{3}$. Then $\mathrm{ord}_3(y) = 1$ and $\mathrm{ord}_{pq}(y) = \mathrm{ord}_{pq}(x) = a$, so $\mathrm{ord}_{3pq}(y) = \mathrm{lcm}(1,\, a) = a$. Further, $\mathrm{ord}_3(y+1)$ $= \mathrm{ord}_3(2) = 2$ and $\mathrm{ord}_{pq}(y+1) = \mathrm{ord}_{pq}(x+1) = b$, so $\mathrm{ord}_{3pq}(y+1) = \mathrm{lcm}(2,\, b) = b$ as $b$ is even.

We now check that $\langle y \rangle \cap \langle y+1 \rangle = \{1\}$. Suppose that $y^i \equiv (y+1)^j \pmod{3pq}$ for some $i$ and $j$ with $0 \le i < a$ and $0 \le j < b$. Then $x^i \equiv (x+1)^j \pmod{pq}$. But $\langle x \rangle \cap \langle x+1 \rangle = \{1\}$ in $\mathbb{Z}_{pq}$, so $i = j = 0$ as required. □

**Note.** For $pq = 35$, 55, 65, 77, 85, 91 and 95, all values $x$ with $1 < x < pq-1$ and $\mathbb{U}_{pq} = \langle x \rangle_a \times \langle x+1 \rangle_b \pmod{pq}$ can be taken in Theorem 31 to generate half of the units of $\mathbb{Z}_n$ where $n$ is one of the values 105, 165, 195, 231, 255, 273 and 285, for which we have $\xi(n) = 4$, 4, 8, 4, 8, 12 and 4 respectively.

**Theorem 32** *Let $n = 3pq$ where $p$ and $q$ are distinct primes greater than 3. Let $x$ be any integer, $1 < x < pq-1$, such that precisely half of the members of $\mathbb{U}_{pq}$ are provided by $\langle x \rangle_a \times \langle x+1 \rangle_b \pmod{pq}$ for some $a$ and $b$, each greater than 1, with $b$*

*odd. Let $k$ be the value, taken from $\{0, 1, 2\}$, such that $x + kpq \equiv 1 \pmod 3$. Then precisely half of the members of $\mathbb{U}_n$ are contained in*

$$\langle x + kpq\rangle_a \times \langle x + kpq + 1\rangle_{2b}\ .$$

*Proof.* Similar to the proof of Theorem 31. □

**Note.** With $pq = 91$, we can obtain half of the members of $\mathbb{U}_{pq}$ from $\langle 73\rangle_{12} \times \langle 74\rangle_3$ and also from $\langle 15\rangle_{12} \times \langle 16\rangle_3$. Thus Theorem 32 shows that we can obtain half of $\mathbb{U}_{273}$ from $\langle 73\rangle_{12} \times \langle 74\rangle_6$ and also from $\langle 106\rangle_{12} \times \langle 107\rangle_6$.

## References

[1] I. Anderson and D. A. Preece, A general approach to constructing power-sequence terraces for $\mathbb{Z}_n$, *Discrete Math.* **38** (2008), 631–644.

[2] N. G. W. H. Beeger, On a new case of the congruence $2^{p-1} = 1$ $(p^2)$, *Messenger Math.* **51** (1922), 149–150.

[3] P. J. Cameron and D. A. Preece, *Notes on Primitive $\lambda$-roots.* Available at `http://www.maths.qmul.ac.uk/~pjc/csgnotes/lambda.pdf` .

[4] P. J. Cameron and D. A. Preece, Three-factor decompositions of $\mathbb{U}_n$ with the three generators in arithmetic progression, arXiv:111.3507v1 [math.NT] 15 Nov 2011 .

[5] R. D. Carmichael, Note on a new number theory function, *Bull. Amer. Math. Soc.* **16** (1909–10), 232–238.

[6] R. D. Carmichael, Generalisations of Euler's $\phi$-function, with applications to Abelian groups, *Quart. J. Math.* **44** (1913), 94–104.

[7] W. Meissner, Über die Teilbarkeit von $2^p - 2$ durch das Quadrat der Primzahl $p = 1093$, *Akad. d. Wiss., Berlin, Sitzungsb.* **35** (1913), 663–667.

[8] D. A. Preece, Daisy chains — a fruitful combinatorial concept, *Australasian J. Combinatorics* **41** (2008), 297–316.

[9] D. A. Preece, Half-cycles and chaplets, *Australasian J. Combinatorics* **43** (2009), 253–280.

[10] D. A. Preece, Daisy chains with three generators, *Australasian J. Combinatorics* **45** (2009), 157–174.

[11] D. A. Preece, Supplementary tables for *Daisy chains with three generators.* Available at `ajc.maths.uq.edu.au/appendices/AJCvol145pp157-174Appendix.pdf` .

[12] D. A. Preece, and E. R. Vaughan, Daisy chains with four generators, *Australasian J. Combinatorics* **49** (2011), 77–93.

[13] A. Wieferich, Zum letzten Fermatschen Theorem, *J. reine angew. Math.* **136** (1909), 293–302.

**Appendix**

**Table 1.** Instances of $\langle x\rangle \times \langle x+1\rangle$ providing all or half of $\mathbb{U}_n$ where $n$ is a prime power, $n < 300$

| $n$ | Theorem | $\mathbb{U}_n$ | half of $\mathbb{U}_n$ |
|---|---|---|---|
| $5^t$ | | – | – |
| $7^u$ | | – | – |
| $9^t$ | 2.8 | $\langle 7\rangle_3 \times \langle 8\rangle_2$ | |
| $11^t$ | 2.1 | $\langle 9\rangle_5 \times \langle 10\rangle_2$ | |
| $13^t$ | 2.4, 2.6 | $\langle 8\rangle_4 \times \langle 9\rangle_3$ | |
| $17^u$ | | – | – |
| $19^t$ | 2.1 | $\langle 17\rangle_9 \times \langle 18\rangle_2$ | |
| $23^u$ | | – | – |
| $25^t$ | 2.8 | $\langle 6\rangle_5 \times \langle 7\rangle_4$ | |
| $27^t$ | 2.10 | $\langle 25\rangle_9 \times \langle 26\rangle_2$ | |
| $29^t$ | 2.4 | $\langle 16\rangle_7 \times \langle 17\rangle_4$ | |
| 31 | 2.7 | | ${\langle 4\rangle_5 \times \langle 5\rangle_3}^*$ |
| $37^t$ | 2.4 | $\langle 6\rangle_4 \times \langle 7\rangle_9$ | |
| $41^u$ | 2.5 | $\langle 37\rangle_5 \times \langle 38\rangle_8$ | ${\langle 9\rangle_4 \times \langle 10\rangle_5}^{\ddagger}$ |
| 43 | 2.7 | | ${\langle 35\rangle_7 \times \langle 36\rangle_3}^*$ |
| $47^u$ | | – | – |
| $49^u$ | 2.9 | | ${\langle 29\rangle_7 \times \langle 30\rangle_3}^{*\ddagger}$ |
| $53^t$ | 2.4 | $\langle 23\rangle_4 \times \langle 24\rangle_{13}$ | |
| $59^t$ | 2.1 | $\langle 57\rangle_{29} \times \langle 58\rangle_2$ | |
| $61^t$ | 2.4 | $\begin{Bmatrix} \langle 20\rangle_5 \times \langle 21\rangle_{12} \\ \langle 11\rangle_4 \times \langle 12\rangle_{15} \end{Bmatrix}$ | |
| $67^t$ | 2.1 | $\langle 65\rangle_{33} \times \langle 66\rangle_2$ | |
| $71^u$ | 2.2 | $\begin{Bmatrix} \langle 45\rangle_7 \times \langle 46\rangle_{10} \\ \langle 25\rangle_5 \times \langle 26\rangle_{14} \end{Bmatrix}$ | |
| 73 | | – | – |
| $79^u$ | 2.7 | | ${\langle 22\rangle_{13} \times \langle 23\rangle_3}^{*\ddagger}$ |
| $81^t$ | 2.10 | $\langle 79\rangle_{27} \times \langle 80\rangle_2$ | |
| $83^t$ | 2.1 | $\langle 81\rangle_{41} \times \langle 82\rangle_2$ | |
| 89 | | $\langle 77\rangle_8 \times \langle 78\rangle_{11}$ | |
| $97^u$ | 2.6 | $\langle 34\rangle_{32} \times \langle 35\rangle_3$ | |

continued . . .

$^*$ does not contain $-1 \pmod{n}$

$^{\ddagger}$ $\langle x\rangle \times \langle x+1\rangle = \langle 2\rangle$

$^t$ 2 is a primitive root of $n$

$^u$ $\mathrm{ord}_n(2) = \phi(n)/2$

**Table 1** [page 2]

| $n$ | Theorem | $\mathbb{U}_n$ | half of $\mathbb{U}_n$ |
|---|---|---|---|
| $101^t$ | 2.4 | $\langle 91\rangle_4 \times \langle 92\rangle_{25}$ | |
| $103^u$ | | – | – |
| $107^t$ | 2.1 | $\langle 105\rangle_{53} \times \langle 106\rangle_2$ | |
| 109 | | – | – |
| 113 | | $\langle 48\rangle_{16} \times \langle 49\rangle_7$ | |
| $121^t$ | 2.8 | $\left\{\begin{array}{c}\langle 119\rangle_{55} \times \langle 120\rangle_2 \\ \langle 111\rangle_{11} \times \langle 112\rangle_{10} \\ \langle 9\rangle_5 \times \langle 10\rangle_{22}\end{array}\right\}$ | |
| $125^t$ | 2.10 | $\langle 56\rangle_{25} \times \langle 57\rangle_4$ | |
| 127 | | – | – |
| $131^t$ | | | $\left\{\begin{array}{c}\left\{\begin{array}{c}\langle 52\rangle_{13} \times \langle 53\rangle_5{}^* \\ \langle 60\rangle_{13} \times \langle 61\rangle_5{}^*\end{array}\right\} \\ \langle 61\rangle_5 \times \langle 62\rangle_{13}{}^*\end{array}\right\}$ |
| $137^u$ | 2.5 | | $\langle 37\rangle_4 \times \langle 38\rangle_{17}{}^{\ddagger}$ |
| $139^t$ | $\left\{\begin{array}{c}2.1,\ 2.2, \\ 2.6\end{array}\right\}$ | $\left\{\begin{array}{c}\langle 137\rangle_{69} \times \langle 138\rangle_2 \\ \left\{\begin{array}{c}\langle 95\rangle_{46} \times \langle 96\rangle_3 \\ \langle 43\rangle_6 \times \langle 44\rangle_{23}\end{array}\right\}\end{array}\right\}$ | |
| $149^t$ | 2.4 | $\langle 104\rangle_{37} \times \langle 105\rangle_4$ | |
| 151 | | – | – |
| 157 | 2.3 | $\langle 107\rangle_{12} \times \langle 108\rangle_{13}$ | $\left\{\begin{array}{c}\langle 143\rangle_{26} \times \langle 144\rangle_3 \\ \langle 13\rangle_6 \times \langle 14\rangle_{13}\end{array}\right\}$ |
| $163^t$ | 2.1 | $\langle 161\rangle_{81} \times \langle 162\rangle_2$ | |
| $167^u$ | | – | – |
| $169^t$ | 2.8 | $\left\{\begin{array}{c}\langle 21\rangle_{52} \times \langle 22\rangle_3 \\ \langle 79\rangle_{13} \times \langle 80\rangle_{12} \\ \langle 99\rangle_4 \times \langle 100\rangle_{39}\end{array}\right\}$ | |
| $173^t$ | 2.4 | $\langle 80\rangle_4 \times \langle 81\rangle_{43}$ | |
| $179^t$ | 2.1 | $\langle 177\rangle_{89} \times \langle 178\rangle_2$ | |
| $181^t$ | 2.4 | $\left\{\begin{array}{c}\langle 161\rangle_{45} \times \langle 162\rangle_4 \\ \langle 73\rangle_9 \times \langle 74\rangle_{20}\end{array}\right\}$ | |
| $191^u$ | 2.2 | $\left\{\begin{array}{c}\left\{\begin{array}{c}\langle 38\rangle_{38} \times \langle 39\rangle_5 \\ \langle 152\rangle_{10} \times \langle 153\rangle_{19}\end{array}\right\} \\ \left\{\begin{array}{c}\langle 6\rangle_{19} \times \langle 7\rangle_{10} \\ \langle 184\rangle_5 \times \langle 185\rangle_{38}\end{array}\right\}\end{array}\right\}$ | |

continued . . .

**Table 1** [page 3]

| $n$ | Theorem | $\mathbb{U}_n$ | half of $\mathbb{U}_n$ |
|---|---|---|---|
| $193^u$ | | $-$ | $-$ |
| $197^t$ | 2.4 | $\langle 182\rangle_{49} \times \langle 183\rangle_4$ | |
| $199^u$ | 2.2 | $\left\{\begin{array}{c}\langle 18\rangle_{11} \times \langle 19\rangle_{18} \\ \langle 180\rangle_{9} \times \langle 181\rangle_{22}\end{array}\right\}$ | |
| $211^t$ | 2.7 | | $\left\{\begin{array}{c}\langle 13\rangle_{35} \times \langle 14\rangle_{3}{}^{*} \\ \langle 54\rangle_{21} \times \langle 55\rangle_{5}{}^{*}\end{array}\right\}$ |
| 223 | 2.2, 2.6 | $\left\{\begin{array}{c}\langle 182\rangle_{74} \times \langle 183\rangle_{3} \\ \langle 40\rangle_{6} \times \langle 41\rangle_{37}\end{array}\right\}$ | |
| $227^t$ | 2.1 | $\langle 225\rangle_{113} \times \langle 226\rangle_2$ | |
| 229 | 2.6 | $\left\{\begin{array}{c}\langle 93\rangle_{76} \times \langle 94\rangle_{3} \\ \langle 17\rangle_{19} \times \langle 18\rangle_{12}\end{array}\right\}$ | |
| 233 | | $\langle 135\rangle_{29} \times \langle 136\rangle_8$ | |
| $239^u$ | 2.2 | $\left\{\begin{array}{c}\langle 23\rangle_{34} \times \langle 24\rangle_{7} \\ \langle 215\rangle_{14} \times \langle 216\rangle_{17}\end{array}\right\}$ | $\langle 100\rangle_7 \times \langle 101\rangle_{17}{}^{*\ddagger}$ |
| 241 | 2.6 | $\left\{\begin{array}{c}\langle 224\rangle_{80} \times \langle 225\rangle_{3} \\ \langle 87\rangle_{5} \times \langle 88\rangle_{48}\end{array}\right\}$ | |
| $243^t$ | 2.10 | $\langle 241\rangle_{81} \times \langle 242\rangle_2$ | |
| 251 | | $-$ | $-$ |
| 257 | | $-$ | $-$ |
| $263^u$ | | $-$ | $-$ |
| $269^t$ | 2.4 | $\langle 81\rangle_{67} \times \langle 82\rangle_4$ | |
| $271^u$ | 2.2 | $\left\{\begin{array}{c}\langle 83\rangle_{27} \times \langle 84\rangle_{10} \\ \langle 187\rangle_{5} \times \langle 188\rangle_{54}\end{array}\right\}$ | |
| 277 | 2.6 | $\langle 159\rangle_{92} \times \langle 160\rangle_3$ | |
| 281 | | $-$ | $-$ |
| 283 | 2.2, 2.6 | $\left\{\begin{array}{c}\langle 43\rangle_{94} \times \langle 44\rangle_{3} \\ \langle 239\rangle_{6} \times \langle 240\rangle_{47}\end{array}\right\}$ | |
| $289^u$ | 2.9 | | $\langle 154\rangle_{17} \times \langle 155\rangle_8$ |
| $293^t$ | 2.4 | $\langle 137\rangle_{73} \times \langle 138\rangle_4$ | |

**Table 2.** Instances of $\langle x\rangle \times \langle x+1\rangle$ providing all or half of $\mathbb{U}_n$ where $n$ satisfies $\xi(n) = 2$, $n < 300$

| $n$ | Theorem | $\mathbb{U}_n$ | half of $\mathbb{U}_n$ |
|---|---|---|---|
| $15^u = 3 \times 5$ | 3.1, 3.9 | $\langle 13\rangle_4 \times \langle 14\rangle_2{}^{\dagger}$ | |
| $21^u = 3 \times 7$ | 3.1, 3.8 | $\langle 19\rangle_6 \times \langle 20\rangle_2{}^{\dagger}$ | |
| $33^u = 3 \times 11$ | 3.3 | | $\langle 31\rangle_5 \times \langle 32\rangle_2{}^{\dagger\ddagger}$ |
| $35^u = 5 \times 7$ | 3.1, 3.7 | $\langle 33\rangle_{12} \times \langle 34\rangle_2{}^{\dagger}$<br>$\langle 26\rangle_6 \times \langle 27\rangle_4{}^{\dagger}$ | |
| $39^u = 3 \times 13$ | 3.1, 3.9 | $\langle 37\rangle_{12} \times \langle 38\rangle_2{}^{\dagger}$<br>$\langle 34\rangle_4 \times \langle 35\rangle_6$ | |
| $45^u = 3^2 \times 5$ | 3.1, 3.6 | $\langle 43\rangle_{12} \times \langle 44\rangle_2{}^{\dagger}$<br>$\langle 28\rangle_4 \times \langle 29\rangle_6{}^{\dagger}$ | $\langle 16\rangle_3 \times \langle 17\rangle_4{}^{*\dagger\ddagger}$ |
| $51 = 3 \times 17$ | 3.2 | | $\langle 49\rangle_8 \times \langle 50\rangle_2{}^{\dagger}$ |
| $55^u = 5 \times 11$ | 3.1, 3.9 | $\langle 53\rangle_{20} \times \langle 54\rangle_2{}^{\dagger}$<br>$\langle 23\rangle_4 \times \langle 24\rangle_{10}{}^{\dagger}$ | $\langle 31\rangle_5 \times \langle 32\rangle_4{}^{*\dagger\ddagger}$ |
| $57^u = 3 \times 19$ | 3.3 | | $\langle 55\rangle_9 \times \langle 56\rangle_2{}^{\dagger\ddagger}$ |
| $69^u = 3 \times 23$ | 3.1, 3.8 | $\langle 67\rangle_{22} \times \langle 68\rangle_2{}^{\dagger}$ | |
| $75^u = 3 \times 5^2$ | 3.1, 3.4 | $\langle 73\rangle_{20} \times \langle 74\rangle_2{}^{\dagger}$<br>$\langle 43\rangle_4 \times \langle 44\rangle_{10}$ | $\langle 31\rangle_5 \times \langle 32\rangle_4{}^{*\ddagger}$ |
| $77^u = 7 \times 11$ | 3.1, 3.8 | $\langle 75\rangle_{30} \times \langle 76\rangle_2{}^{\dagger}$<br>$\langle 12\rangle_6 \times \langle 13\rangle_{10}{}^{\dagger}$ | $\langle 64\rangle_5 \times \langle 65\rangle_6{}^{*\dagger\ddagger}$ |
| $87^u = 3 \times 29$ | 3.1, 3.4,<br>3.9 | $\langle 85\rangle_{28} \times \langle 86\rangle_2{}^{\dagger}$<br>$\langle 70\rangle_4 \times \langle 71\rangle_{14}$ | $\langle 16\rangle_7 \times \langle 17\rangle_4{}^{*\ddagger}$ |
| $93 = 3 \times 31$ | 3.5 | $\langle 88\rangle_6 \times \langle 89\rangle_{10}$ | $\langle 4\rangle_5 \times \langle 5\rangle_6{}^{*}$ |
| $95^u = 5 \times 19$ | 3.1, 3.9 | $\langle 93\rangle_{36} \times \langle 94\rangle_2{}^{\dagger}$<br>$\langle 58\rangle_4 \times \langle 59\rangle_{18}$ | $\langle 36\rangle_9 \times \langle 37\rangle_4{}^{*\dagger\ddagger}$ |

continued...

$^*$ does not include $-1 \pmod{n}$

$^\dagger$ $x(x+1) \equiv 2$ and thus $(x+2)(x-1) \equiv 0 \pmod{n}$

$^\ddagger$ $\langle x\rangle \times \langle x+1\rangle = \langle 2\rangle$

$^u$ $\mathrm{ord}_n(2) = \phi(n)/2$

**Table 2** [page 2]

| $n$ | Theorem | $\mathbb{U}_n$ | half of $\mathbb{U}_n$ |
|---|---|---|---|
| $99^u = 3^2 \times 11$ | 3.6 | | $\langle 97\rangle_{15} \times \langle 98\rangle_2{}^{\dagger\ddagger}$<br>$\langle 64\rangle_5 \times \langle 65\rangle_6{}^{\dagger\ddagger}$<br>$\langle 34\rangle_3 \times \langle 35\rangle_{10}{}^{\dagger\ddagger}$ |
| $111^u = 3 \times 37$ | 3.1, 3.9 | $\langle 109\rangle_{36} \times \langle 110\rangle_2{}^{\dagger}$<br>$\langle 43\rangle_4 \times \langle 44\rangle_{18}$ | |
| $115^u = 5 \times 23$ | 3.1, 3.7 | $\langle 113\rangle_{44} \times \langle 114\rangle_2{}^{\dagger}$<br>$\langle 21\rangle_{22} \times \langle 22\rangle_4{}^{\dagger}$ | |
| $119 \ = 7 \times 17$ | | | $\langle 103\rangle_6 \times \langle 104\rangle_8{}^{\dagger}$ |
| $123 \ = 3 \times 41$ | 3.2, 3.4 | $\langle 85\rangle_8 \times \langle 86\rangle_{10}$ | $\langle 121\rangle_{20} \times \langle 122\rangle_2{}^{\dagger}$<br>$\langle 37\rangle_5 \times \langle 38\rangle_8{}^{*}$ |
| $129 \ = 3 \times 43$ | 3.5 | $\langle 7\rangle_6 \times \langle 8\rangle_{14}$ | $\langle 121\rangle_7 \times \langle 122\rangle_6{}^{*}$ |
| $135^u = 3^3 \times 5$ | 3.1 | $\langle 133\rangle_{36} \times \langle 134\rangle_2{}^{\dagger}$<br>$\langle 28\rangle_4 \times \langle 29\rangle_{18}{}^{\dagger}$ | $\langle 106\rangle_9 \times \langle 107\rangle_4{}^{*\dagger\ddagger}$ |
| $141^u = 3 \times 47$ | 3.1, 3.8 | $\langle 139\rangle_{46} \times \langle 140\rangle_2{}^{\dagger}$ | |
| $143^u = 11 \times 13$ | 3.1, 3.9 | $\langle 141\rangle_{60} \times \langle 142\rangle_2{}^{\dagger}$<br>$\langle 89\rangle_{12} \times \langle 90\rangle_{10}{}^{\dagger}$<br>$\langle 34\rangle_4 \times \langle 35\rangle_{30}$ | $\langle 53\rangle_5 \times \langle 54\rangle_{12}{}^{*\dagger\ddagger}$ |
| $147^u = 3 \times 7^2$ | 3.1, 3.5 | $\langle 145\rangle_{42} \times \langle 146\rangle_2{}^{\dagger}$<br>$\langle 19\rangle_6 \times \langle 20\rangle_{14}$ | $\langle 127\rangle_7 \times \langle 128\rangle_6{}^{*\ddagger}$ |
| $153 \ = 3^2 \times 17$ | 3.2 | | $\langle 151\rangle_{24} \times \langle 152\rangle_2{}^{\dagger}$ |
| $155 \ = 5 \times 31$ | 3.5 | $\langle 88\rangle_{12} \times \langle 89\rangle_{10}$ | $\langle 66\rangle_5 \times \langle 67\rangle_{12}{}^{*}$ |
| $159^u = 3 \times 53$ | 3.1, 3.9 | $\langle 157\rangle_{52} \times \langle 158\rangle_2{}^{\dagger}$<br>$\langle 76\rangle_4 \times \langle 77\rangle_{26}$ | |
| $161 \ = 7 \times 23$ | | – | – |
| $175^u = 5^2 \times 7$ | 3.1, 3.4 | $\langle 173\rangle_{60} \times \langle 174\rangle_2{}^{\dagger}$<br>$\langle 68\rangle_{12} \times \langle 69\rangle_{10}$ | $\langle 106\rangle_5 \times \langle 107\rangle_{12}{}^{*\ddagger}$ |

continued . . .

**Table 2** [page 3]

| $n$ | | Theorem | $\mathbb{U}_n$ | half of $\mathbb{U}_n$ |
|---|---|---|---|---|
| $177^u$ | $= 3 \times 59$ | 3.3 | | $\langle 175\rangle_{29} \times \langle 176\rangle_{2}{}^{\dagger\ddagger}$ |
| $183^u$ | $= 3 \times 61$ | 3.1, 3.4,<br>3.9 | $\langle 181\rangle_{60} \times \langle 182\rangle_{2}{}^{\dagger}$<br>$\langle 40\rangle_{12} \times \langle 41\rangle_{10}$<br>$\langle 133\rangle_{4} \times \langle 134\rangle_{30}$ | $\langle 142\rangle_{5} \times \langle 143\rangle_{12}{}^{*\ddagger}$ |
| $187$ | $= 11 \times 17$ | 3.2 | | $\langle 185\rangle_{40} \times \langle 186\rangle_{2}{}^{\dagger}$<br>$\langle 100\rangle_{8} \times \langle 101\rangle_{10}{}^{\dagger}$ |
| $201^u$ | $= 3 \times 67$ | 3.3 | | $\langle 199\rangle_{33} \times \langle 200\rangle_{2}{}^{\dagger\ddagger}$ |
| $203^u$ | $= 7 \times 29$ | 3.1, 3.4,<br>3.7 | $\langle 201\rangle_{84} \times \langle 202\rangle_{2}{}^{\dagger}$<br>$\langle 12\rangle_{12} \times \langle 13\rangle_{14}$<br>$\langle 117\rangle_{6} \times \langle 118\rangle_{28}{}^{\dagger}$ | $\langle 190\rangle_{7} \times \langle 191\rangle_{12}{}^{*\ddagger}$ |
| $207^u$ | $= 3^2 \times 23$ | 3.1, 3.6 | $\langle 205\rangle_{66} \times \langle 206\rangle_{2}{}^{\dagger}$<br>$\langle 136\rangle_{22} \times \langle 137\rangle_{6}{}^{\dagger}$ | $\langle 70\rangle_{3} \times \langle 71\rangle_{22}{}^{*\dagger\ddagger}$ |
| $209^u$ | $= 11 \times 19$ | 3.3 | | $\langle 207\rangle_{45} \times \langle 208\rangle_{2}{}^{\dagger\ddagger}$<br>$\langle 188\rangle_{9} \times \langle 189\rangle_{10}{}^{\dagger\ddagger}$<br>$\langle 20\rangle_{5} \times \langle 21\rangle_{18}{}^{\dagger\ddagger}$ |
| $213^u$ | $= 3 \times 71$ | 3.1, 3.4,<br>3.8 | $\langle 211\rangle_{70} \times \langle 212\rangle_{2}{}^{\dagger}$ | $\langle 187\rangle_{7} \times \langle 188\rangle_{10}$<br>$\langle 25\rangle_{5} \times \langle 26\rangle_{14}$ |
| $215$ | $= 5 \times 43$ | 3.5 | $\langle 93\rangle_{12} \times \langle 94\rangle_{14}$ | $\langle 121\rangle_{7} \times \langle 122\rangle_{12}{}^{*}$ |
| $219$ | $= 3 \times 73$ | | – | – |
| $225^u$ | $= 3^2 \times 5^2$ | 3.1 | $\langle 223\rangle_{60} \times \langle 224\rangle_{2}{}^{\dagger}$<br>$\langle 73\rangle_{20} \times \langle 74\rangle_{6}{}^{\dagger}$<br>$\langle 43\rangle_{12} \times \langle 44\rangle_{10}$<br>$\langle 118\rangle_{4} \times \langle 119\rangle_{30}$ | $\langle 106\rangle_{15} \times \langle 107\rangle_{4}{}^{*\ddagger}$<br>$\langle 181\rangle_{5} \times \langle 182\rangle_{12}{}^{*\ddagger}$<br>$\langle 151\rangle_{3} \times \langle 152\rangle_{20}{}^{*\dagger\ddagger}$ |
| $235^u$ | $= 5 \times 47$ | 3.1, 3.7 | $\langle 233\rangle_{92} \times \langle 234\rangle_{2}{}^{\dagger}$<br>$\langle 186\rangle_{46} \times \langle 187\rangle_{4}{}^{\dagger}$ | |

continued . . .

**Table 2** [page 4]

| $n$ | | Theorem | $\mathbb{U}_n$ | half of $\mathbb{U}_n$ |
|---|---|---|---|---|
| $237^u$ | $= 3 \times 79$ | 3.1, 3.5,<br>3.8 | $\langle 235\rangle_{78} \times \langle 236\rangle_{2}{}^{\dagger}$<br>$\langle 214\rangle_{6} \times \langle 215\rangle_{26}$ | $\langle 22\rangle_{13} \times \langle 23\rangle_{6}{}^{*\ddagger}$ |
| $245^u$ | $= 5 \times 7^2$ | 3.1, 3.5 | $\langle 243\rangle_{84} \times \langle 244\rangle_{2}{}^{\dagger}$<br>$\langle 68\rangle_{12} \times \langle 69\rangle_{14}$ | $\langle 176\rangle_{7} \times \langle 177\rangle_{12}{}^{*\ddagger}$ |
| $249^u$ | $= 3 \times 83$ | 3.3 | | $\langle 247\rangle_{41} \times \langle 248\rangle_{2}{}^{\dagger\ddagger}$ |
| $253^u$ | $= 11 \times 23$ | 3.1, 3.8 | $\langle 251\rangle_{110} \times \langle 252\rangle_{2}{}^{\dagger}$<br>$\langle 67\rangle_{22} \times \langle 68\rangle_{10}{}^{\dagger}$ | $\langle 185\rangle_{5} \times \langle 186\rangle_{22}{}^{*\dagger\ddagger}$ |
| $261^u$ | $= 3^2 \times 29$ | 3.1, 3.6 | $\langle 259\rangle_{84} \times \langle 260\rangle_{2}{}^{\dagger}$<br>$\langle 172\rangle_{28} \times \langle 173\rangle_{6}{}^{\dagger}$<br>$\langle 70\rangle_{12} \times \langle 71\rangle_{14}$<br>$\langle 244\rangle_{4} \times \langle 245\rangle_{20}$ | $\langle 16\rangle_{21} \times \langle 17\rangle_{4}{}^{*\ddagger}$<br>$\langle 190\rangle_{7} \times \langle 191\rangle_{12}{}^{*\ddagger}$<br>$\langle 88\rangle_{3} \times \langle 89\rangle_{28}{}^{*\dagger\ddagger}$ |
| $267$ | $= 3 \times 89$ | | $\langle 166\rangle_{8} \times \langle 167\rangle_{22}$ | |
| $287$ | $= 7 \times 41$ | 3.4 | $\langle 208\rangle_{24} \times \langle 209\rangle_{10}$ | $\langle 285\rangle_{60} \times \langle 286\rangle_{2}{}^{\dagger}$<br>$\langle 236\rangle_{30} \times \langle 237\rangle_{4}$<br>$\langle 124\rangle_{6} \times \langle 125\rangle_{20}$<br>$\langle 78\rangle_{5} \times \langle 79\rangle_{24}{}^{*}$ |
| $291$ | $= 3 \times 97$ | 3.2 | $\langle 34\rangle_{32} \times \langle 35\rangle_{6}$ | $\langle 289\rangle_{48} \times \langle 290\rangle_{2}{}^{\dagger}$ |
| $295^u$ | $= 5 \times 59$ | 3.1, 3.9 | $\langle 293\rangle_{116} \times \langle 294\rangle_{2}{}^{\dagger}$<br>$\langle 178\rangle_{4} \times \langle 179\rangle_{58}{}^{\dagger}$ | $\langle 116\rangle_{29} \times \langle 117\rangle_{4}{}^{*\dagger\ddagger}$ |
| $297^u$ | $= 3^3 \times 11$ | 3.3 | | $\langle 295\rangle_{45} \times \langle 296\rangle_{2}{}^{\dagger\ddagger}$<br>$\langle 133\rangle_{9} \times \langle 134\rangle_{10}{}^{\dagger\ddagger}$<br>$\langle 163\rangle_{5} \times \langle 164\rangle_{18}{}^{\dagger\ddagger}$ |
| $299^u$ | $= 13 \times 23$ | 3.1, 3.7 | $\langle 297\rangle_{132} \times \langle 298\rangle_{2}{}^{\dagger}$<br>$\langle 251\rangle_{66} \times \langle 252\rangle_{4}$<br>$\langle 274\rangle_{22} \times \langle 275\rangle_{12}{}^{\dagger}$ | $\langle 47\rangle_{4} \times \langle 48\rangle_{33}{}^{*}$ |

**Table 3.** Instances of $\langle x\rangle \times \langle x+1\rangle$ providing all or half of $\mathbb{U}_n$ where $n$ satisfies $\xi(n) > 2$, $n < 300$

| $n$ | $\xi(n)$ | Theorem | $\mathbb{U}_n$ | half of $\mathbb{U}_n$ |
|---|---|---|---|---|
| 63<br>$=3^2\times 7$ | 6 | 3.6 | $\langle x\rangle_6 \times \langle x+1\rangle_6$<br>$x = 52, 40^\dagger;\ 10, 19^\dagger$ | $\langle x\rangle_3 \times \langle x+1\rangle_6$<br>$x = 22^{*\dagger}, 43^{*\dagger};\ 4, 16;$<br>$25, 58;\ 46, 37$ |
| 65<br>$=5\times 13$ | 4 | 3.4, 4.1 | $\langle x\rangle_{12} \times \langle x+1\rangle_4$<br>$x = 17, 46;\ 33, 43;\ 37, 11^\dagger$<br>$\langle x\rangle_4 \times \langle x+1\rangle_{12}$<br>$x = 47, 18;\ 31, 21;\ 27, 53^\dagger$ | $\langle 56\rangle_6 \times \langle 57\rangle_4$<br>$\langle 8\rangle_4 \times \langle 9\rangle_6$ |
| 85<br>$=5\times 17$ | 4 | 4.2 | $\langle x\rangle_{16} \times \langle x+1\rangle_4$<br>$x = 37, 46;\ 12, 71$<br>$\langle x\rangle_4 \times \langle x+1\rangle_{16}$<br>$x = 47, 38;\ 72, 13$ | $\langle x\rangle_8 \times \langle x+1\rangle_4$<br>$x = 32, 66^\dagger$<br>$\langle x\rangle_4 \times \langle x+1\rangle_8$<br>$x = 52, 18^\dagger$ |
| 91<br>$=7\times 13$ | 6 | 3.7, 4.5 | $\langle x\rangle_{12} \times \langle x+1\rangle_6$<br>$x = 37, 11;\ 47, 54;$<br>$60, 2;\ 67, 86$<br>$\langle x\rangle_6 \times \langle x+1\rangle_{12}$<br>$x = 17, 75;\ 66, 40^\dagger$ | $\langle x\rangle_{12} \times \langle x+1\rangle_3$<br>$x = 73^*, 15^*$<br>$\langle x\rangle_6 \times \langle x+1\rangle_6$<br>$x = 3, 61;\ 87, 68$<br>$\langle x\rangle_3 \times \langle x+1\rangle_{12}$<br>$x = 53^*, 79^*$ |
| 105<br>$=3\times 5\times 7$ | 4 | 3.2, 7.1 | $-^\#$ | $\langle 103\rangle_{12} \times \langle 104\rangle_2{}^\dagger$<br>$\langle 61\rangle_6 \times \langle 62\rangle_4{}^{*\dagger}$<br>$\langle 43\rangle_4 \times \langle 44\rangle_6{}^{*\dagger}$ |
| 117<br>$=3^2\times 13$ | 6 | 3.6 | $\langle x\rangle_{12} \times \langle x+1\rangle_6$<br>$x = 76^\dagger, 37^\dagger;\ 34, 106;\ 28, 112$ | $\langle x\rangle_3 \times \langle x+1\rangle_{12}$<br>$x = 40^{*\dagger}, 79^{*\dagger}$ |

continued...

$^*$ does not include $-1 \pmod{n}$
$^\dagger$ $x(x+1) \equiv 2$ and thus $(x+2)(x-1) \equiv 0 \pmod{n}$
$^\#$ Impossible, as $n$ has 3 distinct prime factors

**Table 3** [page 2]

| $n$ | $\xi(n)$ | Theorem | $\mathbb{U}_n$ | half of $\mathbb{U}_n$ |
|---|---|---|---|---|
| 133<br>$=7\times 19$ | 6 | 3.8, 4.4 | $\langle x\rangle_{18}\times\langle x+1\rangle_6$<br>$x=17,67,86$<br>$\langle x\rangle_6\times\langle x+1\rangle_{18}$<br>$x=115,96^\dagger;\ 65,88;$<br>$46,107;\ 31,103$ | $\langle x\rangle_{18}\times\langle x+1\rangle_3$<br>$x=101^*,29^*;\ 10$<br>$\langle x\rangle_9\times\langle x+1\rangle_6$<br>$x=36^{*\dagger},44^*,25^*;\ 93,74$<br>$\langle 122\rangle_6\times\langle 123\rangle_9$<br>$\langle x\rangle_3\times\langle x+1\rangle_{18}$<br>$x=39,58$ |
| 145<br>$=5\times 29$ | 4 | 4.1 | $\langle x\rangle_{28}\times\langle x+1\rangle_4$<br>$x=132,11;\ 98,103;$<br>$27,56^\dagger$<br>$\langle x\rangle_4\times\langle x+1\rangle_{28}$<br>$x=12,133;\ 46,41;$<br>$117,88^\dagger$ | – |
| 165<br>$=3\times 5\times 11$ | 4 | 3.2, 7.1 | $-^{\#}$ | $\langle 163\rangle_{20}\times\langle 164\rangle_2{}^\dagger$<br>$\langle 133\rangle_4\times\langle 134\rangle_{10}{}^\dagger$ |
| 171<br>$=3^2\times 19$ | 6 | 3.6 | $\langle x\rangle_{18}\times\langle x+1\rangle_6$<br>$x=10,67$<br>$\langle x\rangle_6\times\langle x+1\rangle_{18}$<br>$x=160,31;\ 103,88$ | $\langle x\rangle_9\times\langle x+1\rangle_6$<br>$x=139^*,82^*;\ 112^\dagger,55^\dagger$<br>$\langle x\rangle_3\times\langle x+1\rangle_{18}$<br>$x=58^\dagger,115^\dagger$ |
| 185<br>$=5\times 37$ | 4 | 3.4, 4.1 | $\langle x\rangle_{36}\times\langle x+1\rangle_4$<br>$x=67,116;\ 178,153;$<br>$72,146^\dagger$<br>$\langle x\rangle_4\times\langle x+1\rangle_{36}$<br>$x=117,68;\ 6,31;$<br>$112,38^\dagger$ | $\langle 141\rangle_{18}\times\langle 142\rangle_4$<br>$\langle 43\rangle_4\times\langle 44\rangle_{18}$ |
| 189<br>$=3^3\times 7$ | 6 | – | $\langle x\rangle_{18}\times\langle x+1\rangle_6$<br>$x=52,115,178$<br>$\langle x\rangle_6\times\langle x+1\rangle_{18}$<br>$x=136,82;\ 73,145;$<br>$10,19$ | $\langle x\rangle_9\times\langle x+1\rangle_6$<br>$x=106^{*\dagger},43^{*\dagger},169^{*\dagger};$<br>$151,142;\ 88,16;\ 25,79$<br>$\langle x\rangle_3\times\langle x+1\rangle_{18}$<br>$x=37,46;\ 100,172;$<br>$163,109$ |

continued...

**Table 3** [page 3]

| $n$ | $\xi(n)$ | Theorem | $\mathbb{U}_n$ | half of $\mathbb{U}_n$ |
|---|---|---|---|---|
| 195<br>$=3\times5\times13$ | 8 | 7.1 | $-^{\#}$ | $\langle x\rangle_{12}\times\langle x+1\rangle_4$<br>$x=82^*,46^*;\ 163^*,43^*;$<br>$37^*,76^{*\dagger}$<br>$\langle x\rangle_4\times\langle x+1\rangle_{12}$<br>$x=112^*,148^*;\ 31^*,151^*;$<br>$157^*,118^{*\dagger}$ |
| 205<br>$=5\times41$ | 4 | 4.3 | $\langle x\rangle_{20}\times\langle x+1\rangle_8$<br>$x=2,43;\ 37,78$<br>$\langle x\rangle_8\times\langle x+1\rangle_{20}$<br>$x=202,161;\ 167,126$ | $\langle x\rangle_{20}\times\langle x+1\rangle_4$<br>$x=72,131;\ 113,8;$<br>$162,121^{\dagger}$<br>$\langle 3\rangle_8\times\langle 4\rangle_{10}$<br>$\langle x\rangle_4\times\langle x+1\rangle_{20}$<br>$x=132,73;\ 91,196;$<br>$42,83^{\dagger}$ |
| 217<br>$=7\times31$ | 6 | 4.4 | $\langle x\rangle_{30}\times\langle x+1\rangle_6$<br>$x=86,179;\ 117$<br>$\langle x\rangle_6\times\langle x+1\rangle_{30}$<br>$x=150,68;\ 130,212;$<br>$37,88$ | $\langle x\rangle_{30}\times\langle x+1\rangle_3$<br>$x=66^*,148^*$<br>$\langle x\rangle_{15}\times\langle x+1\rangle_6$<br>$x=128^*,4^*$<br>$\langle 99\rangle_6\times\langle 100\rangle_{15}{}^*$ |
| 221<br>$=13\times17$ | 4 | 4.2 | $\langle x\rangle_{48}\times\langle x+1\rangle_4$<br>$x=20,199;\ 46,173$<br>$\langle x\rangle_{16}\times\langle x+1\rangle_{12}$<br>$x=105,122;\ 131$<br>$\langle x\rangle_{12}\times\langle x+1\rangle_{16}$<br>$x=115,98;\ 89$<br>$\langle x\rangle_4\times\langle x+1\rangle_{48}$<br>$x=200,21;\ 174,47$ | $\langle x\rangle_{24}\times\langle x+1\rangle_4$<br>$x=134,202$<br>$\langle x\rangle_{12}\times\langle x+1\rangle_8$<br>$x=137,154^{\dagger}$<br>$\langle x\rangle_8\times\langle x+1\rangle_{12}$<br>$x=83,66^{\dagger}$<br>$\langle x\rangle_4\times\langle x+1\rangle_{24}$<br>$x=86,18$ |
| 231<br>$=3\times7\times11$ | 4 | 3.2, 7.1 | $-^{\#}$ | $\langle 229\rangle_{30}\times\langle 230\rangle_2{}^{\dagger}$<br>$\langle 166\rangle_6\times\langle 167\rangle_{10}{}^{\dagger}$ |

continued...

**Table 3** [page 4]

| $n$ | $\xi(n)$ | Theorem | $\mathbb{U}_n$ | half of $\mathbb{U}_n$ |
|---|---|---|---|---|
| 247<br>=13×19 | 6 | 3.9, 4.5 | $\langle x\rangle_{36}\times\langle x+1\rangle_6$<br>$x=93,112$<br>$\langle 105\rangle_{18}\times\langle 106\rangle_{12}$<br>$\langle x\rangle_{12}\times\langle x+1\rangle_{18}$<br>$x=50,115^\dagger;\ 210$<br>$\langle x\rangle_6\times\langle x+1\rangle_{36}$<br>$x=69,179;\ 88,160$ | $\langle x\rangle_{36}\times\langle x+1\rangle_3$<br>$x=177^*,67^*;\ 158^*,86^*$<br>$\langle x\rangle_{18}\times\langle x+1\rangle_6$<br>$x=29,48$<br>$\langle 236\rangle_{12}\times\langle 237\rangle_9{}^*$<br>$\langle x\rangle_9\times\langle x+1\rangle_{12}$<br>$x=196^*,131^{*\dagger}$<br>$\langle x\rangle_6\times\langle x+1\rangle_{18}$<br>$x=217,107;\ 198,126$ |
| 255<br>=3×5×17 | 8 | 7.1 | $-^\#$ | $\langle x\rangle_{16}\times\langle x+1\rangle_4$<br>$x=37^*,46^*;\ 97^*,241^*$<br>$\langle x\rangle_4\times\langle x+1\rangle_{16}$<br>$x=217^*,208^*;\ 157^*,13^*$ |
| 259<br>=7×37 | 6 | 3.7, 4.6 | $\langle x\rangle_{36}\times\langle x+1\rangle_6$<br>$x=72,109$<br>$\langle x\rangle_{18}\times\langle x+1\rangle_{12}$<br>$x=178,192,213$<br>$\langle x\rangle_{12}\times\langle x+1\rangle_{18}$<br>$x=156,177$<br>$\langle x\rangle_6\times\langle x+1\rangle_{36}$<br>$x=38,75^\dagger$ | $\langle x\rangle_{18}\times\langle x+1\rangle_6$<br>$x=247,25$<br>$\langle x\rangle_{12}\times\langle x+1\rangle_9$<br>$x=80^*,45^*$<br>$\langle x\rangle_9\times\langle x+1\rangle_{12}$<br>$x=44^*,81^*,155^*$<br>$\langle x\rangle_6\times\langle x+1\rangle_{18}$<br>$x=11,212;\ 233,249;$<br>$101,159$<br>$\langle x\rangle_3\times\langle x+1\rangle_{36}$<br>$x=186^*,149^*$ |
| 265<br>=5×53 | 4 | 3.4, 4.1 | $\langle x\rangle_{52}\times\langle x+1\rangle_4$<br>$x=82,181;\ 188,128;$<br>$157,51^\dagger$<br>$\langle x\rangle_4\times\langle x+1\rangle_{52}$<br>$x=182,83;\ 76,136;$<br>$107,213^\dagger$ | $\langle 241\rangle_{26}\times\langle 242\rangle_4$<br>$\langle 23\rangle_4\times\langle 24\rangle_{26}$ |

continued...

**Table 3** [page 5]

| $n$ | $\xi(n)$ | Theorem | $\mathbb{U}_n$ | half of $\mathbb{U}_n$ |
|---|---|---|---|---|
| 273<br>$=3\times 7\times 13$ | 12 | 7.1, 7.2 | $-^{\#}$ | $\langle x\rangle_{12}\times\langle x+1\rangle_{6}$<br>$x=73^{*},106^{*};\ 37,193;$<br>$229,145;\ 151,184;$<br>$67,268;\ 115^{*},232^{*\dagger}$<br>$\langle x\rangle_{6}\times\langle x+1\rangle_{12}$<br>$x=199,166;\ 157^{*},40^{*\dagger}$ |
| 275<br>$=5^2\times 11$ | 10 | 3.4, 6.1 | $\langle x\rangle_{20}\times\langle x+1\rangle_{10}$<br>$x=188,258;\ 28,18;$<br>$23^{\dagger},148;\ 248,73;$<br>$133,38;\ 193,128;$<br>$78,93;\ -,-;$<br>$-,-;\ 138,183;$<br>$218,53;\ 163,108$<br>$\langle x\rangle_{10}\times\langle x+1\rangle_{20}$<br>$x=206,271;\ 116,211;$<br>$151,51;\ 226,101;$<br>$96,106;\ 61,266;$<br>$261,216;\ 6,46;$<br>$-,-;171,156$ | $\langle x\rangle_{5}\times\langle x+1\rangle_{20}$<br>$x=86^{*},16^{*};\ 246^{*},256^{*};$<br>$251^{*\dagger},126^{*};\ 26^{*},201^{*};$<br>$141^{*},236^{*};\ 81^{*},146^{*};$<br>$196^{*},181^{*};\ -,-;$<br>$-,-;\ 136^{*},91^{*};$<br>$56^{*},221^{*};\ 111^{*},166^{*}$ |
| 279<br>$=3^2\times 31$ | 6 | – | $\langle x\rangle_{30}\times\langle x+1\rangle_{6}$<br>$x=55,241$<br>$\langle x\rangle_{6}\times\langle x+1\rangle_{30}$<br>$x=223,274;\ 37,181$ | $\langle x\rangle_{15}\times\langle x+1\rangle_{6}$<br>$x=4^{*},97^{*}$ |
| 285<br>$=3\times 5\times 19$ | 4 | 3.2, 7.1 | $-^{\#}$ | $\langle 283\rangle_{36}\times\langle 284\rangle_{2}{}^{\dagger}$<br>$\langle 58\rangle_{4}\times\langle 59\rangle_{18}{}^{\dagger}$ |

**Table 4.** In the range $0 < n < 2000$, Theorem 24 and Corollary 25 cover parameter sets as follows, where we take $q > p$:

| $n$ | $p$ | $q$ | $x_1,\ x_2$ | $z_1,\ \ z_2$ |
|---:|---:|---:|---:|---:|
| 133 | 7 | 19 | 31,103 | 88, 46 |
| 217 | 7 | 31 | 150, 68 | 88, 130 |
| 301 | 7 | 43 | 136,166 | 179, 123 |
| 469 | 7 | $67^\dagger$ | 164,306 | – |
| 553 | 7 | 79 | 451,103 | 214, 340 |
| 589 | 19 | 31 | 316,274 | – |
| 721 | 7 | $103^\dagger$ | 150,572 | – |
| 817 | 19 | 43 | 639,179 | – |
| 889 | 7 | 127 | 108,782 | 235, 655 |
| 973 | 7 | 139 | $^\ddagger$ | 599, 375 |
| 1057 | 7 | $151^\dagger$ | 1025, 33 | – |
| 1141 | 7 | 163 | 920,222 | 431, 711 |
| 1333 | 31 | 43 | 781,553 | – |
| 1393 | 7 | 199 | 1102,292 | 704, 690 |
| 1477 | 7 | 211 | 619,859 | 830, 648 |
| 1501 | 19 | 79 | 1209,293 | – |
| 1561 | 7 | 223 | $^\ddagger$ | 263,1299 |
| $1897^*$ | 7 | 271 | $^\ddagger$ | – |
| 1957 | 19 | $103^\dagger$ | 1190,768 | – |
| 1981 | 7 | 283 | $^\ddagger$ | 522,1460 |

$^*$ 3 is not a primitive $\lambda$-root of $n$

$^\dagger$ $\mathrm{ord}_q(3) = (q-1)/3$

$^\ddagger$ fails; congruence $x^2 \equiv x - 1$ is satisfied by $x = 3^{\mu/6}$ and by $x = 3^{5\mu/6}$