1. Find the decimal expansion of $\frac{1}{p}$ when

(a) $p = 17$  (b) $p = 23$.

Use your results to find $\text{ord}_{17}(10)$ and $\text{ord}_{23}(10)$.

**Solution**

(a) For $p = 17$, we have

\[
\begin{align*}
10 &= a_1 \times 17 + r_1, \text{ so } a_1 = 0 \text{ and } r_1 = 10, \\
100 &= a_2 \times 17 + r_2 = 5 \times 17 + 15, \\
150 &= a_3 \times 17 + r_3 = 8 \times 17 + 14, \\
140 &= a_4 \times 17 + r_4 = 8 \times 17 + 4, \\
40 &= a_5 \times 17 + r_5 = 2 \times 17 + 6, \\
60 &= a_6 \times 17 + r_6 = 3 \times 17 + 9, \\
90 &= a_7 \times 17 + r_7 = 5 \times 17 + 5, \\
50 &= a_8 \times 17 + r_8 = 2 \times 17 + 16, \\
160 &= a_9 \times 17 + r_9 = 9 \times 17 + 7, \\
70 &= a_{10} \times 17 + r_{10} = 4 \times 17 + 2, \\
20 &= a_{11} \times 17 + r_{11} = 1 \times 17 + 3, \\
30 &= a_{12} \times 17 + r_{12} = 1 \times 17 + 13, \\
130 &= a_{13} \times 17 + r_{13} = 7 \times 17 + 11, \\
110 &= a_{14} \times 17 + r_{14} = 6 \times 17 + 8, \\
80 &= a_{15} \times 17 + r_{15} = 4 \times 17 + 12, \\
120 &= a_{16} \times 17 + r_{16} = 7 \times 17 + 1. \\
\end{align*}
\]

Therefore $\text{ord}_{17}(10) = 16$ (as $r_{16} = 1$) and $\frac{1}{17} = 0.0588235294117647$. We can also deduce that 10 is a generator of $\mathbb{Z}_{17}^*$.

(b) For $p = 23$,

\[
\begin{align*}
10 &= a_1 \times 23 + r_1, \text{ so } a_1 = 0 \text{ and } r_1 = 10, \\
100 &= a_2 \times 23 + r_2 = 4 \times 23 + 8, \\
80 &= a_3 \times 23 + r_3 = 3 \times 23 + 11, \\
110 &= a_4 \times 23 + r_4 = 4 \times 23 + 18, \\
180 &= a_5 \times 23 + r_5 = 7 \times 23 + 19, \\
190 &= a_6 \times 23 + r_6 = 8 \times 23 + 6, \\
60 &= a_7 \times 23 + r_7 = 2 \times 23 + 14, \\
140 &= a_8 \times 23 + r_8 = 6 \times 23 + 2, \\
20 &= a_9 \times 23 + r_9 = 0 \times 23 + 20, \\
200 &= a_{10} \times 23 + r_{10} = 8 \times 23 + 16. \\
\end{align*}
\]
160 = a_{11} \times 23 + r_{11} = 6 \times 23 + 22,
220 = a_{12} \times 23 + r_{12} = 9 \times 23 + 13,
130 = a_{13} \times 23 + r_{13} = 5 \times 23 + 15,
150 = a_{14} \times 23 + r_{14} = 6 \times 23 + 12,
120 = a_{15} \times 23 + r_{15} = 5 \times 23 + 5,
50 = a_{16} \times 23 + r_{16} = 2 \times 23 + 4,
40 = a_{17} \times 23 + r_{17} = 1 \times 23 + 17,
170 = a_{18} \times 23 + r_{18} = 7 \times 23 + 9,
90 = a_{19} \times 23 + r_{19} = 3 \times 23 + 21,
210 = a_{20} \times 23 + r_{20} = 9 \times 23 + 3,
30 = a_{21} \times 23 + r_{21} = 1 \times 23 + 7,
70 = a_{22} \times 23 + r_{22} = 3 \times 23 + 1.

Therefore \( \text{ord}_{23}(10) = 22 \) (as \( r_{22} = 1 \)) and \( \frac{1}{23} = 0.0434782608695652173913 \). We can also deduce that 10 is a generator of \( \mathbb{Z}_{23}^* \).

2. Show that \( x = \frac{1}{2^a 5^b} = 0.a_1 a_2 \ldots a_k \) where \( k = \max(a, b) \).

Solution

Suppose that \( a \leq b \) Then \( 10^b x = 2^{b-a} \) and it has a decimal expansion \( a_0 + a_1 10 + a_2 10^2 + \ldots + a_\ell 10^\ell \), where \( 0 \leq a_i \leq 9, a_0 \neq 0 \) because \( 10^b x = 2^{b-a} \) is not a multiple of 10 and \( \ell \leq b - a \). Hence

\[
x = \frac{a_0}{10^b} + \frac{a_1}{10^{b-1}} + \ldots + \frac{a_\ell}{10^{b-(\ell-1)}} + \frac{a_\ell}{10^{b-\ell}},
\]

and \( x \) has a finite decimal expansion of length \( b = \max(a, b) \).

The argument when \( a > b \) is exactly similar. Then \( 10^a x = 5^{a-b} = b_0 + b_1 10 + b_2 10^2 + \ldots + b_m 10^m \) where \( 0 \leq b_i \leq 9, b_0 \neq 0 \) because \( 10^a x \) is not a multiple of 10 and \( m \leq a - b \). Hence

\[
x = \frac{b_0}{10^a} + \frac{b_1}{10^{a-1}} + \ldots + \frac{b_m}{10^{a-(m-1)}} + \frac{b_m}{10^{a-m}}.
\]

This time \( x \) has a finite decimal expansion of length \( a = \max(a, b) \).

3. Evaluate \( A_n = \prod_{x \in \mathbb{Z}_n^*} x \) when \( n = 14 \) and \( n = 21 \). Show that if \( x^2 = 1 \in \mathbb{Z}_n^* \) then \((-x)^2 = 1 \).

Hence if \( n > 2 \) there is always an even number \( 2k \) of elements \( x \in \mathbb{Z}_n^* \) such that \( x^2 = 1 \). Show that \( \prod_{x \in \mathbb{Z}_n^*} x = (-1)^k \), where \( 2k \) is the number of elements \( x \) such that \( x^2 = 1 \).

Solution

\( \mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\} \) and \( A_{14} = 1.3.5.9.11.13 = 13 = (-1)^1 \).

\( \mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 9, 10, 11, 13, 16, 17, 19, 20\} \) and

\[
A = 1.2.4.5.8.10(-10)(-8)(-5)(-4)(-2)(-1)
= 1.(-1)2.(-10)4.(-5)5(-4)10.2.8.(-8)
= (-1)^2
= 1.
\]
In general, first note that if \( x^2 = 1 \), then \((-x)^2 = 1\) and \( x \neq -x \), since then \( 2x = 0 \in \mathbb{Z}_n \).
If \( n \) is odd, we must have \( x = 0 \), while if \( n = 2k \) then \( x = k \) and \( k^2 \equiv 1 \pmod{2k} \) implies that \( k^2 = k \ell + 1 \) and so \( k = 1 \) and \( n = 2 \), a contradiction.
So the elements \( x \) such that \( x^2 = 1 \) come in pairs if \( n > 2 \) and so there is an even number of them. Hence, in evaluating the product \( \prod_{x \in \mathbb{Z}_n^*} x \), we can cancel those terms \( x \) and \( y \) for which \( xy = 1 \) and \( x \neq y \). This leaves the terms \( x \) such that \( x = x^{-1} \). These come in pairs \( x \) and \(-x\) as we have remarked. But then we can cancel \( x \) and \(-x\) and are left with \(-1\) for each of the \( k \) pairs. Thus \( \prod_{x \in \mathbb{Z}_n^*} x = (-1)^k \).

4. (a) Find all the powers of 2 in \( \mathbb{Z}_{31} \).
(b) Find all the powers of 3 in \( \mathbb{Z}_{31} \).
(c) Find \( \text{ord}_{31}(2) \), \( \text{ord}_{31}(3) \).

**Solution**
(a) The powers of 2 are:
\[
2, \ 2^2 = 4, \ 2^3 = 8, \ 2^4 = 16, \ 2^5 = 32 = 1,
\]
and hence
\[
2^6 = 2^5 \times 2^1 = 2, \ 2^7 = 2^2 = 4
\]
and so on. Every power of 2 right up to \( 2^{30} \) is either 1, 2, 4, 8 or 16.
(b) The powers of 3 are:
\[
\begin{array}{cccccccccccc}
k & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\
3^k & 3 & 9 & -4 & -12 & -5 & -15 & -14 & -2 & -6 & 13 & 8 & -7 & 10 & -1 \\
\end{array}
\]
(c) In \( \mathbb{Z}_{31} \), \( \text{ord}_{31}(2) = 5 \) and \( \text{ord}_{31}(3) = 30 \).

5. Find \( \varphi(18) \), \( \varphi(30) \), \( \varphi(60) \).

**Solution**
The method is as follows: write down all the numbers from 1 to 18.
\[
1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \\
10 \ 11 \ 12 \ 13 \ 14 \ 15 \ 16 \ 17 \ 18.
\]
Cross out the numbers which have a factor (greater than 1) in common with 18.
\[
1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \\
10 \ 11 \ 12 \ 13 \ 14 \ 15 \ 16 \ 17 \ 18.
\]
We are left with the numbers
1, 5, 7, 11, 13, 17
and so \( \varphi(18) = 6 \)
Similarly, \( \varphi(30) = 8 \), the number of elements in the set
\{1, 7, 11, 13, 17, 19, 23, 29\}.
\( \varphi(60) = 16 \), the number of elements in the set
\{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59\}.
6. Find generators, if they exist, of the following:

\[ \mathbb{Z}_{13}^*, \mathbb{Z}_{17}^*, \mathbb{Z}_{31}^*, \mathbb{Z}_{15}^*, \mathbb{Z}_{22}^*, \mathbb{Z}_{25}^*, \mathbb{Z}_{16}^*, \mathbb{Z}_{43}^*. \]

**Solution**

Just one generator is given, where it exists. (Other answers are possible.)

(a) In \( \mathbb{Z}_{13}^* \), 2 is a generator. \( (\varphi(13) = 12) \)

(b) In \( \mathbb{Z}_{17}^* \), 3 is a generator. \( (\varphi(17) = 16) \)

(c) In \( \mathbb{Z}_{31}^* \), 3 is a generator. \( (\varphi(31) = 32) \)

(d) There is no generator for \( \mathbb{Z}_{15}^* \). \( (\varphi(15) = 8.) \) \( (1^1 = 2^4 = 4^2 = 7^1 = 11^2 = 13^1 = 14^2 = 1, \) so each element has order less than \( \varphi(15) \).)

(e) 7 is a generator for \( \mathbb{Z}_{22}^* \). \( (\varphi(22) = 10.) \)

(f) 2 is a generator for \( \mathbb{Z}_{25}^* \). \( (\varphi(25) = 20.) \)

(g) There is no generator for \( \mathbb{Z}_{16}^* \). \( (1^1 = 3^4 = 5^4 = 7^2 = 9^2 = 11^4 = 13^4 = 15^2 = 1 \in \mathbb{Z}_{16}.) \)

(h) 3 is a generator for \( \mathbb{Z}_{43}^* \). \( (\varphi(43) = 42.) \)

7. Find all elements \( x \) of \( \mathbb{Z}_{10}^*, \mathbb{Z}_{12}^*, \mathbb{Z}_{15}^*, \mathbb{Z}_{21}^*, \mathbb{Z}_{24}^* \) and \( \mathbb{Z}_{60}^* \) such that \( x^2 = 1 \).

**Solution**

The elements are

\[
\begin{align*}
\mathbb{Z}_{10}^* & \quad 1 \quad 9 \\
\mathbb{Z}_{12}^* & \quad 1 \quad 5 \quad 7 \quad 11 \\
\mathbb{Z}_{15}^* & \quad 1 \quad 4 \quad 11 \quad 14 \\
\mathbb{Z}_{21}^* & \quad 1 \quad 8 \quad 13 \quad 20 \\
\mathbb{Z}_{24}^* & \quad 1 \quad 5 \quad 7 \quad 11 \quad 13 \quad 17 \quad 19 \quad 23 \\
\mathbb{Z}_{60}^* & \quad 1 \quad 11 \quad 19 \quad 29 \quad 31 \quad 41 \quad 49.
\end{align*}
\]

Note that every element in both \( \mathbb{Z}_{12}^* \) and \( \mathbb{Z}_{24}^* \) satisfies \( x^2 = 1 \).