# WEB3CLUBS FOUNDATION LIMITED

Course Instructor: DR. Cyprian Omukhwaya Sakwa
PHONE: +254723584205   Email: cypriansakwa@gmail.com

# Foundational Mathematics for Web3 Builders

## Lecture 3

**April 25, 2024**

**Theorem 10**

*Let $m$ bbe a positive integer. Then prove that*

a) *For any integer $a$ we have $a \equiv a(\bmod m)$*

b) *If $a \equiv b(\bmod m)$ then $b \equiv a(\bmod m)$*

c) *If $a \equiv b(\bmod m)$ and $b \equiv c(\bmod m)$ then $a \equiv c(\bmod m)$.*

d) *If $a \equiv c(\bmod m)$ and $b \equiv d(\bmod m)$ then*

   *i)* $(a+b) \equiv (c+d)(\bmod m)$  *ii)* $(a \cdot b) \equiv (c \cdot d)(\bmod m)$

**Definition 11**

The set $\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, 3, \cdots m-1\}$ is called a ring of integers modulo $m$.

The $\mathbb{Z}/m\mathbb{Z}$ is the quotient ring of $\mathbb{Z}$ by the principal ideal $m\mathbb{Z}$, and the numbers $\{0, 1, 2, 3, \cdots m-1\}$ are actually coset representatives for the congruence classes that comprise the elements of $\mathbb{Z}/m\mathbb{Z}$.

This notion of of ideals and general quotient rings is quite useful in a number of contexts which will be explored later.

To perform addition or multiplication in $\mathbb{Z}/m\mathbb{Z}$ we always divide the result by $m$ and take the remainder in order to obtain an element in $\mathbb{Z}/m\mathbb{Z}$.
Let us study the following addition and multiplication Cayley tables of $\mathbb{Z}/5\mathbb{Z}$ modulo $5$.

| $+$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

a: Addition table for $\mathbb{Z}/5\mathbb{Z}$

| $\times$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

b: Multiplication table for $\mathbb{Z}/5\mathbb{Z}$

Table 1

# 1.7 Linear Congruence

Consider the linear congruence

$$ax \equiv b \pmod{m} \tag{1}$$

where $a, b, m$ are integers with $m > 0$.
By a solution of equation (1) we mean an integer $x = x_1$ for which $m \mid (ax_1 - b)$.
Note that if $x_1$ is a solution of equation (1) then $x_1 + km$ for $k \in \mathbb{Z}$ is another solution of equation (1).
**Note:** An equation $ax \equiv b \pmod{m}$ has a solution if $\gcd(a, m)$ divides $b$. In this case, if $d = \gcd(a, m)$ and $d \mid b$ then the congruence equation has $d$ solutions. This congruence equation has no solution if $d \nmid b$.

### Example 32

Solve the following linear congruence equations.

a) $5x \equiv 3 (\bmod 8)$

b) $6x \equiv 4 (\bmod 9)$

c) $6x \equiv 8 (\bmod 10)$

d) $3x + 2 \equiv 8 (\bmod 10)$

e) $6x - 3 \equiv 5 + 2x (\bmod 10)$

f) $\frac{2}{3}x \equiv 4 (\bmod 7)$

### Solution

Since the moduli is relatively small, we will find solutions by testing. Later on we will see how to use extended Euclid's Algorithm to find solutions to such congruence equations.

## Solution (conti...)

a) Here $\gcd(5,8) = 1$ and $1$ divides $3$ hence the equation has a unique solution. Let us test $0, 1, 2, 3, \cdots 7$ to find the solution.

$$\begin{aligned}
5(0) &= 0 \not\equiv 3 \pmod 8 & \qquad 5(4) &= 4 \not\equiv 3 \pmod 8 \\
5(1) &= 5 \not\equiv 3 \pmod 8 & \qquad 5(5) &= 1 \not\equiv 3 \pmod 8 \\
5(2) &= 2 \not\equiv 3 \pmod 8 & \qquad 5(6) &= 6 \not\equiv 3 \pmod 8 \\
5(3) &= 7 \not\equiv 3 \pmod 8 & \qquad 5(7) &= 3 \equiv 3 \pmod 8
\end{aligned}$$

Thus the unique solution is $x = 7$

b) The $\gcd(6,9) = 3$ but $3 \nmid 4$ and so the congruence equation has no solution.

## Solution (conti...)

c) Here $\gcd(6,10) = 2$ and $2 \mid 8$ hence the equation has two solutions. Let us test $0, 1, 2, 3, \cdots 9$ to find the solutions.

$$\begin{array}{ll}
6(0) = 0 \not\equiv 8 (\bmod 10) & 6(5) = 0 \not\equiv 8 (\bmod 10) \\
6(1) = 6 \not\equiv 8 (\bmod 10) & 6(6) = 6 \not\equiv 8 (\bmod 10) \\
6(2) = 2 \not\equiv 8 (\bmod 10) & 6(7) = 2 \not\equiv 8 (\bmod 10) \\
6(3) = 8 \equiv 8 (\bmod 10) & 6(8) = 8 \equiv 8 (\bmod 10) \\
6(4) = 4 \not\equiv 8 (\bmod 10) & 6(9) = 4 \not\equiv 8 (\bmod 10)
\end{array}$$

Thus the two solutions are $x_1 = 3$ and $x_2 = 8$

We work with congruence relations modulo $m$ much as with ordinary equalities. That is, we add to, subtract from, or multiply both sides of a congruence modulo $m$ by the same integer; also, if $b$ is congruent to $a$ modulo $m$ we may substitute $b$ for $a$.

## Solution (conti...)

d) First we subtract $2$ on both sides to get $3x \equiv 6 \pmod{10}$. Here, $\gcd(3, 10) = 1$ and $1$ divides $6$ and so the equation has one solution. Now test $0, 1, 2, \cdots 9$ to find the solution.

$$3(0) = 0 \not\equiv 6 \pmod{10}$$
$$3(1) = 3 \not\equiv 6 \pmod{10}$$
$$3(2) = 6 \equiv 6 \pmod{10}$$
$$3(3) = 9 \not\equiv 6 \pmod{10}$$
$$3(4) = 2 \not\equiv 6 \pmod{10}$$
$$3(5) = 5 \not\equiv 6 \pmod{10}$$
$$3(6) = 8 \not\equiv 6 \pmod{10}$$
$$3(7) = 1 \not\equiv 6 \pmod{10}$$
$$3(8) = 4 \not\equiv 6 \pmod{10}$$
$$3(9) = 7 \not\equiv 6 \pmod{10}$$

Thus the solution is $x = 2$

## Solution (conti...)

e) Collect like terms. $6x - 2x \equiv 5 + 3 \pmod{10}$ which becomes $4x \equiv 8 \pmod{10}$. The $\gcd(4, 10) = 2$ and $2 \mid 8$ hence equation has 2 solutions. Now test $0, 1, 2, \cdots 9$ to find the solution.

$$\begin{array}{ll}
4(0) = 0 \not\equiv 8 \pmod{10} & 4(5) = 0 \not\equiv 8 \pmod{10} \\
4(1) = 4 \not\equiv 8 \pmod{10} & 4(6) = 4 \not\equiv 8 \pmod{10} \\
4(2) = 8 \equiv 8 \pmod{10} & 4(7) = 8 \equiv 8 \pmod{10} \\
4(3) = 2 \not\equiv 8 \pmod{10} & 4(8) = 2 \not\equiv 8 \pmod{10} \\
4(4) = 6 \not\equiv 8 \pmod{10} & 4(9) = 6 \not\equiv 8 \pmod{10}
\end{array}$$

The solutions are $x_1 = 2$ and $x_2 = 7$

## Solution (conti...)

f) To work with fractions $a/d$modulo $m$ the denominator must be relatively prime to $m$.
Simplify $\frac{2}{3}x \equiv 4 \pmod 7$ to get $2x \equiv 12 \pmod 7$ or $2x \equiv 5 \pmod 7$. Now, $\gcd(2,7) = 1$ and so there is one solution. Test $0, 1, 2, \cdots 6$ to find the solution.

$$2(0) = 0 \not\equiv 5 \pmod 7$$
$$2(1) = 2 \not\equiv 5 \pmod 7$$
$$2(2) = 4 \not\equiv 5 \pmod 7$$
$$2(3) = 6 \not\equiv 5 \pmod 7$$

$$2(4) = 1 \not\equiv 5 \pmod 7$$
$$2(5) = 3 \not\equiv 5 \pmod 7$$
$$2(6) = 5 \equiv 5 \pmod 7$$

Thus the solution is $x = 6$.

# 1.8 Solution of Linear Congruences Using Euclid's Algorithm

## Example 33

Find the least positive integer $x$ for which

$$53x \equiv 1 \bmod 93$$

## Solution

First, $\gcd(93, 53) = 1$ and $1$ divides $1$ and the equation has $1$ solution.

By Euclid's algorithm algorithm we have

$93 = 53(1) + 40$

$53 = 40(1) + 13$

$40 = 13(3) + 1$

$13 = 1(13) + 0$

## Solution (conti...)

Now solve for the $\gcd$.

$1 = 40 - 13(3) = 40 - [53 - 40(1)](3) = 40 - 53(3) + 40(3)$

$= -53(3) + 40(4) = -53(3) + [93 - 53(1)](4) = -53(3) + 93(4) - 53($

$= 93(4) + 53(-7)$

Thus $1 = 93(4) + 53(-7)$ and therefore modulo $93$ gives

$53(-7) \equiv 1 \bmod 93$.

Thus $x = -7$ is a solution. We could also give this answer as $x = 86$ since $86$ is the least positive number congruent to $-7 \bmod 93$. So, $x = 86$ is the required answer.

## Example 34

Find integer $x$ for which $7x \equiv 13 \bmod 19$

## Solution

$\gcd(19, 7) = 1$ and so equation has $1$ solution.

By Euclid's algorithm algorithm we have

$$19 = 7(2) + 5$$

$$7 = 5(1) + 2$$

$$5 = 2(2) + 1$$

$$2 = 1(2) + 0$$

We solve for $\gcd$

$$1 = 5 - 2(2) = 5 - [7 - 5(1)](2) = 5 - 7(2) + 5(2) = -7(2) + 5(3)$$

$$= -7(2) + [19 - 7(2)](3) = -7(2) + 19(3) - 7(6)$$

$$= 19(3) + 7(-8)$$

That is, $1 = 19(3) + 7(-8)$.

### Solution (conti...)

Since we require $13 = 19(n) + 7(x)$ for some $n \in \mathbb{Z}$, we multiply $1 = 19(3) + 7(-8)$ by 13 to get

$13 = 19(3 \times 13) + 7(-8 \times 13)$ which we compute $\bmod 19$ to get

$13 = 19(1) + 7(10)$

Thus, $x = 10$

### Example 35

Solve $4043n \equiv 27 (\bmod 166361)$

### Solution

Here, $\gcd(166361, 4043) = 13$ but $13 \nmid 27$. Hence the congruence has no solution.

## Example 36

Find all solutions to $15x \equiv 9 \pmod{57}$

## Solution

Here $\gcd(57, 15) = 3$ and $3 \mid 9$ so the equation has three solutions. First divide entire equation and $\bmod 57$ by the $\gcd$ which is $3$ to get

$$5x \equiv 3 \pmod{19}. \tag{2}$$

We first solve equation (2) by Euclidean algorithm.

$$19 = 5(3) + 4$$

$$5 = 4(1) + 1$$

$$4 = 1(4) + 0$$

Now solve for $\gcd$

$$1 = 5 - 4(1) = 5 - [19 - 5(3)](1) = 5 - 19(1) + 5(3)$$

$$= 19(-1) + 5(4)$$

Hence $1 = 19(-1) + 5(4)$.

## Solution (conti...)

To solve equation (2) we multiply $1 = 19(-1) + 5(4)$ by $3$ and compute $\bmod 19$ to get $3 = 19(-3) + 5(12)$ 0r $3 = 19(16) + 5(12)$. Thus $x_1 = 12$ is a solution to our original equation. To get the other solutions we add the new modulus $19$ to $x_1 = 12$ twice. We can also obtain the results using $x = 12 + kn$ where $k = 19$ and $n = \{0, 1, 2\}$.

Thus, $x_1 = 12, \ x_2 = 31, \ x_3 = 50$ are the required solutions to the original equation.

## Example 37

Find all solutions to $1456x \equiv 284 (\bmod 3060)$

## Solution

Here $\gcd(3060, 1456) = 4$ and $4 \mid 284$ so the equation has four solutions.

First divide entire equation and $\bmod 3060$ by the $\gcd$ which is $4$ to get

$$364x \equiv 71 (\bmod 765). \tag{3}$$

We first solve equation (3) by Euclidean algorithm.

$$765 = 364(2) + 37$$

$$364 = 37(9) + 31$$

$$37 = 31(1) + 6$$

$$31 = 6(5) + 1$$

$$6 = 1(6) + 0$$

## Solution (conti...)

Now solve for $\gcd$

$$1 = 31 - 6(5) = 31 - [37 - 31(1)](5)$$

$$= -37(5) + 31(6) = -37(5) + [364 - 37(9)](6)$$

$$= 364(6) - 37(59) = 364(6) - [765 - 364(2)](59)$$

$$= 765(-59) + 364(124)$$

Hence $1 = 765(-59) + 364(124)$.

To solve equation (3) we multiply

$1 = 765(-59) + 364(124)$ by 71 and compute $\bmod 765$ to get

$71 = 765(401) + 364(389)$.

Thus $x_1 = 389$ is a solution to our original equation.

To get the other solutions we add the new modulus 765 to $x_1 = 389$ thrice. We can also get there results using $x = 389 + kn$ where $k = 765$ and $n = \{0, 1, 2, 3\}$.

Thus, $x_1 = 389,\ x_2 = 1154,\ x_3 = 1919, x_4 = 2684$ are the required solutions to the original equation.

## Example 38

1. Find all incongruent solutions to each of the following congruences.

   a) $8x \equiv 3(\mathrm{mod} 15)$ b) $x^2 \equiv 1 \bmod 8$

## Solution

a) Using Euclidean Algorithm we get

$$\begin{aligned} 15 &= 8(1) + 7 \\ 8 &= 7(1) + 1 \\ 7 &= 1(7) + 0 \end{aligned}$$

Thus $1 = 8 - 7(1) = 8 - [15 - 8(1)](1)$

$$= 8 - 15(1) + 8(1) = 15(-1) + 8(2)$$

So $1 = 15(-1) + 8(2)$. Multiplying this by $3$ we get $3 \equiv 15(-3) + 8(6)$ so that $x = 6$.

## Solution (conti...)

b)

a) Try integers $0, 1, 2, \cdots, 7$.

$0^2 = 0 \not\equiv 1 \mod 8$

$1^2 = 1 \equiv 1 \mod 8$

$2^2 = 4 \not\equiv 1 \mod 8$

$3^2 = 9 \equiv 1 \mod 8$

$4^2 = 0 \not\equiv 1 \mod 8$

$5^2 = 25 \equiv 1 \mod 8$

$6^2 = 36 \not\equiv 1 \mod 8$

$7^2 = 49 \equiv 1 \mod 8$

Thus, $x = 1, 3, 5, 7 \mod 8$

## Exercise 3

1. Find all incongruent solutions to each of the following congruences.

   a) $6x \equiv 3(\mod 15)$

   b) $66x \equiv 100(\mod 121)$

   c) $x^2 \equiv 2 \bmod 7$

   d) $x^2 \equiv 3 \bmod 7$

2. Determine the number of incongruent solutions for each of the following congruences. You need not write down the actual solutions.

   a) $72x \equiv 94(\mod 200)$

   b) $4183x \equiv 5781(\mod 15087)$

   c) $1537x \equiv 100(\mod 6731)$

## Exercise (conti...)

3. Write a program that solves the congruence

   $$ax \equiv c \pmod m.$$

   [If $\gcd(a, m)$ does not divide $c$, return an error message and the value of $\gcd(a, m)$.] Test your program by finding all of the solutions to the congruences in question (2) above.

# 1.9 Finding Inverses in Modular Arithmetic

**Definition 12**

If $b$ is a solution to the congruence $ax \equiv 1 (\bmod m)$ then $b$ is the multiplicative inverse of $a$ modulo $m$ and so we say that $a$ is invertible.

Note that $a$ in $ax \equiv 1 (\bmod m)$ is invertible only if $a$ and $m$ are coprime. That is, if $\gcd(m, a) = 1$.
We can use the extended Euclid's algorithm to find inverses in modular arithmetic.

## Example 39

Find $7^{-1} \bmod 19$

## Solution

By Euclid's algorithm algorithm we have

$19 = 7(2) + 5$

$7 = 5(1) + 2$

$5 = 2(2) + 1$

$2 = 1(2) + 0$

We solve for $\gcd$

$$1 = 5 - 2(2) = 5 - [7 - 5(1)](2) = 5 - 7(2) + 5(2) = -7(2) + 5(3)$$
$$= -7(2) + [19 - 7(2)](3) = -7(2) + 19(3) - 7(6)$$
$$= 19(3) + 7(-8)$$

That is, $1 = 19(3) + 7(-8)$.

Thus, $7^{-1} = -8 \equiv 11 \bmod 19$

## Example 40

Solve $364x \equiv 1 \bmod 765$

## Solution

This question wants us to find $364^{-1} \bmod 765$

$$765 = 364(2) + 37$$

$$364 = 37(9) + 31$$

$$37 = 31(1) + 6$$

$$31 = 6(5) + 1$$

$$6 = 1(6) + 0$$

Now solve for $\gcd$

$1 = 31 - 6(5) = 31 - [37 - 31(1)](5)$

$= -37(5) + 31(6) = -37(5) + [364 - 37(9)](6)$

$= 364(6) - 37(59) = 364(6) - [765 - 364(2)](59)$

$= 765(-59) + 364(124)$

Hence $1 = 765(-59) + 364(124)$. Thus $x = 124$

## 1.10 Solution of Congruence Equations Using Inverses

If $b$ is the multiplicative inverse of $a \bmod m$ then we can solve $ax = c \bmod m$ by multiplying both sides by $b$ to get $x \equiv bax \equiv bc \bmod m$.

**Example 41**

Solve $7x \equiv 3 \bmod 19$

**Solution**

From example 39 on page 77, we found that $7^{-1} \bmod 19 = 11$. Thus, multiply both sides of $7x \equiv 3 \bmod 19$ by 11 to get $7(11)x \equiv 3(11) \bmod 19$ which gives $x \equiv 14 \bmod 19$

**Example 42**

Solve $8x \equiv 12 (\bmod 26)$

## Solution

Since $\gcd(26, 8) = 2$ and $2 \mid 12$, the equation has two solutions. First divide the whole equation by $\gcd$ which is $2$ to obtain

$$4x \equiv 6 (\bmod 13) \tag{4}$$

Now, by Euclid's algorithm,

$$13 = 4(3) + 1$$

$$4 = 1(4) + 0$$

Solving for $1$ in the first equation we get $1 = 13 - 4(3)$
Thus $4^{-1} \mod 13 = -3 \equiv 10 \mod 13$.
Therefore multiply both sides of equation (4) by $10$ and reduce $\bmod 13$ to get
$4 \cdot 10x \equiv 6 \cdot 10 \bmod 13$ which gives $x \equiv 8 \bmod 13$.
Thus, $x_1 = 8$ is a solution to the original equation.
And $x_2 = 8 + 13 = 21$

## Example 43

Find all solutions to $51x \equiv 6 \bmod 87$

## Solution

The $\gcd(87, 51) = 3$ and $3 \mid 6$ thus the equation has three solutions. First divide the whole equation by $\gcd$ which is $3$ to obtain

$$17x \equiv 2 (\bmod 29) \tag{5}$$

Now, by Euclid's algorithm,

$$
\begin{aligned}
29 &= 17(1) + 12 \\
17 &= 12(1) + 5 \\
12 &= 5(2) + 2 \\
5 &= 2(2) + 1 \\
2 &= 1(2) + 0
\end{aligned}
$$

### Solution (conti...)

Solving for $1$ in the second last equation we get

$$1 = 5 - 2(2) = 5 - [12 - 5(2)](2)$$
$$= -12(2) + 5(5) = -12(2) + [17 - 12(1)](5)$$
$$= 17(5) - 12(7) = 17(5) - [29 - 17(1)](7)$$
$$= -29(7) + 17(12)$$

Thus $1 = 29(-7) + 17(12)$ so that $17^{-1} \bmod 29 = 12$ Therefore multiply both sides of equation (5) by $12$ and reduce $\bmod 29$ to get $17 \cdot 12x \equiv 2 \cdot 12 \bmod 29$ which gives $x \equiv 24 \bmod 29$.

Thus, $x_1 = 24$ is a solution to the original equation.

And $x_2 = 24 + 29 = 53,\ x_3 = 53 + 29 = 82$ are the other solutions.

Recall that to work with fractions $a/d$modulo $m$ the denominator must be relatively prime to $m$.

### Example 44

Solve $\frac{5}{7}x \equiv 12 \bmod 19$

### Solution

$\frac{5}{7}x \equiv 12 \bmod 19 \Rightarrow 5x \equiv 8 \bmod 19$

Since $\gcd(19,5) = 1$ and $1$ divides $8$ the equation has a solution.

Let us find $5^{-1} \bmod 19$

$$19 = 5(3) + 4$$

$$5 = 4(1) + 1$$

$$4 = 1(4) + 0$$

Now solve for $1$

$1 = 5 - 4(1) = 5 - [19 - 5(3)](1) = 19(-1) + 5(4)$

Thus, $5^{-1} \bmod 19 = 4.$ Now multiply both sides of $5x \equiv 8 \bmod 19$ by $4$ to get $x \equiv 13 \bmod 19$

As stated earlier, $a \in \mathbb{Z}$ has an inverse modulo $m$ if $\gcd(a, m) = 1$. Numbers that have inverses are called units. Let $n > 1$, the set of all units is denoted by

$$U(n) = \{a \in U(n) : \gcd(a, n) = 1\}$$

The set $U(n)$ is called the group of units modulo $m$. That is, it is a group of nonzero integers in modulo $m$ less than $m$ but relatively prime to $m$. It forms a group under multiplication. Study the following Cayley table for $U(5)$ and $U(8)$ for emphasize.

| $\cdot$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

a: Multiplication table for $U(5)$

| $\cdot$ | 1 | 3 | 5 | 7 |
|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 |
| 3 | 3 | 1 | 7 | 5 |
| 5 | 5 | 7 | 1 | 3 |
| 7 | 7 | 5 | 3 | 1 |

b: Multiplication table for $U(8)$

Table 2

### Example 45

The group of units modulo $24$ is $U(24) = \{1, 5, 7, 11, 13, 17, 19, 23\}$

To know how many elements are in the unit group modulo $m$ we use the Euler's phi function (also sometimes known as Euler's totient function).

### Definition 13

Euler phi function, denoted $\phi(n)$, is the number of positive integers less than $n$ which are relatively prime to $n$

Clearly, if $n > 1$ then $\phi(n)$ is the number of elements in $U(n)$ and $\phi(1) = 1$. It is easy to see that $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, $\phi(13) = 12$, $\phi(14) = 6$ and so on. Therefore, elements are in the unit group $U(n)$ is given by $|U(n)| = \phi(n)$.

The following table gives $\phi(n)$ for $n = 1, 2, 3, \cdots, 14$.

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\phi(n)$ | 1 | 1 | 2 | 2 | 4 | 2 | 6 | 4 | 6 | 4 | 10 | 4 | 12 | 6 |

In general, if $p$ is a prime number, $\phi(p) = p - 1$

If $n$ is a positive integer with prime factors $p_1,\ p_2,\ p_3,\ \cdots,\ p_k$ then $\phi(n) = (1 - \frac{1}{p_1})(1 - \frac{1}{p_2})(1 - \frac{1}{p_3}) \cdots (1 - \frac{1}{p_k})n$.

**Example 46**

Find the number of units modulo $4900$.

**Solution**

The number of units in $U(n)$ is given by $\phi(n)$.

Since $4900 = 2^2 \times 5^2 \times 7^2$, we have

$$\phi(4900) = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right)4900$$

$$= \frac{1}{2} \times \frac{4}{5} \times \frac{6}{7} \times 4900 = 1680$$

## Example 47

Denote the Euler phi function by $\phi(n)$. Find $\phi(19)$, $\phi(840)$ and $\phi(930)$.

## Solution

Since 19 is prime, $\phi(19) = 19 - 1 = 18$

$$\begin{aligned}\phi(840) &= \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} \times \frac{6}{7} \times 840 \\ &= 192\end{aligned}$$

$$\begin{aligned}\phi(930) &= \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} \times \frac{30}{31} \times 930 \\ &= 240\end{aligned}$$

In the next section we turn our focus on a reasonably efficient method of computing powers of integers and inverses modulo $p$ where $p$ is prime.