Multiplicative Inverses Modulo n

Any positive integer that is less than n and relatively prime to n has a multiplicative inverse modulo n. This is a consequence of the Euclidean algorithm. We will see in the example below why this must be so. Any positive integer that is less than n and not relatively prime to n does not have a multiplicative inverse modulo n.

Example: find the multiplicative Inverse of 17 mod 43

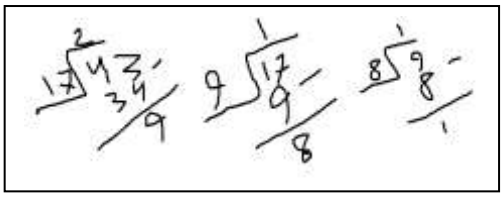
17^{-1} mod 43 =38

Find GCD (17, 43)

43=17*2+9 → 9=43-17*2

17=9*1+8 →8=17-9*1

9=8*1+1 →1=9-8



So, GCD (17, 43) = 1

Now, do the "backward part" of the algorithm (this is often called the "extended Euclidean algorithm)– expressing 1 as a combination of 17 and 43.

1=9-8 →8=17-9*1

1=9-17+9

1=2*9-17→ 9=43-17*2

1=2(43-17*2)-17

1=2*43-4*17-17

2*43 mod 43=0

1=0-5*17

1= -5*17

-5 mod 43 =38 → -5+43=38

X=38

For prove

17*38 mod 43=1

646 mod 43=1

Example: find the multiplicative Inverse of 15 mod 26 $\mathbf{15^{-1} \bmod 26 = 7}$
Solution: First, do the "forward part" of the Euclidean algorithm – finding the GCD.

$26 = 1\times15 + 11 \rightarrow$ A $11=26-15*1$
$15 = 1\times11 + 4 \rightarrow$ B $4=15-11*1$
$11 = 2 \times 4 + 3 \rightarrow$ C $3= 11- 2*4$
$4 = 1\times 3 + 1 \rightarrow$ D $1= 4-3*1$

So, GCD (15, 26) = 1.

Now, do the "backward part" of the algorithm (this is often called the "extended Euclidean algorithm)– expressing 1 as a combination of 15 and 26.

$1 = 4 - 1\times 3$ from D
$1 = 4 - 1\times (11 - 2 \times 4)$ from C
$1=4-1\times11+2 \times 4$
$1 = 3\times 4 - 1\times11$ from B
$1 = 3\times (15 - 1\times11) - 1\times11$
$1 = 3\times15 - 4 \times11$ from A
$1 = 3\times15 - 4 \times (26 - 1\times15)$
$1 = 3\times15 - 4 \times26 + 4\times15 \rightarrow 3\times15 + 4\times15 == 7 \times15$
$1 = 7 \times15 - 4 \times 26$

So, $1 = 7 \times15 - 4 \times 26$.

Finally, "go mod 26." Because 26 = 0 mod 26, when we "go mod 26," the equation $1 = 7 \times15 - 4 \times 26$ becomes the congruence $1 = 7 \times15 \bmod 26$. So, the inverse of 15 modulo 26 is 7

To find $11^7 \bmod 13$, we can proceed as follows:

$$11^2 = 121 \equiv 4 \pmod{13}$$
$$11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$$
$$11^7 = 11 \times 11^2 \times 11^4$$
$$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 \pmod{13}$$

$X = a^{p-2} \bmod p$ P must be Prime

$15^{-1} \bmod 17 = 8$ 17 must be Prime

$15^{17-2} \bmod 17$

$15^{15} \bmod 17$

$15^5 * 15^5 * 15^5 \bmod 17$

$15^5 = 759375 \bmod 17 = 2$

→759375 / 17=44669.1176→44669*17=759373→759375-759373=2

2 * 2 * 2=8

Sul2:

$15^{-1} \bmod 17 = 8$

$X = a^{p-2} \bmod p$ P must be Prime

$15^{-1} \bmod 17 = 8$ 17 must be Prime

$15^{17-2} \bmod 17$

$15^{15} \bmod 17$

$15^4 * 15^4 * 15^4 * 15^3 \bmod 17$

$(15^2)^2 * (15^2)^2 * (15^2)^2 * 15 * 15 * 15$

$15^4 = 4^2 = 16$

16 *16*16*15*15*15= 13824000

13824000 / 17= 813176.4705

17* 813176=13823992

13824000-13823992=8

Sul3:

15^{-1} mod 17 =8

17+17=34+1 / 15=2.3

34+17=51+1 / 15=3.4

51+17=68+1 / 15=4.6

68+17=85+1 / 15= 5.7

85+17=102+1 / 15=6.86

102+17=119+1 / 15= 8

Example: find the multiplicative Inverse of 13 mod 25

The requirement is a should be relatively prime to b, i.e., gcd(a, b) = 1.

Consider $gcd(13, 25)$:

$$\begin{array}{lcll} 25 & = & 1 \times 13 + 12 & gcd(13, 12) \quad (A) \\ 13 & = & 1 \times 12 + 1 & gcd(12, 1) \quad (B) \\ 12 & = & 12 \times 1 + 0 & gcd(1, 0) \end{array}$$

Table: Determine $gcd(13, 25)$

$$\begin{array}{rl} 1 = 13 - 1 \times 12 & From(B) \\ 1 = 13 - 1 \times (25 - 1 \times 13) & From(A) \\ 1 = 2 \times 13 - 1 \times 25 & \\ 1 = 2 \times 13 + (-1) \times 25 & Simplification \end{array}$$

It is easy to see now, 2 is inverse of 13 mod 25.

Find 35−1 mod 96 using Extended Euclidean algorithm

$$96 = 35 \times 2 + 26$$
$$35 = 26 \times 1 + 9$$
$$26 = 9 \times 2 + 8$$
$$9 = 8 \times 1 + 1$$

Thus $GCD(96, 35) = 1$ and the inverse exists.

$$1 = 9 - 8 \times 1$$
$$1 = 9 - (26 - 9 \times 2) \times 1 = 9 \times 3 - 26 \times 1$$
$$1 = (35 - 26 \times 1) \times 3 - 26 \times 1 = 35 \times 3 - 26 \times 4$$
$$1 = 35 \times 3 - (96 - 35 \times 2) \times 4 = 35 \times 11 - 96 \times 4$$

Hence we have $35^{-1} \bmod 96 = 11 \bmod 96 = 11$.

(and the inverse of 7 modulo 26 is 15).

To find the multiplicative inverse of 15 modulo 26, we need to find a number b such that $15 \times b \equiv 1 \pmod{26}$.

We can use the Extended Euclidean Algorithm to find the inverse, or we can use trial and error.

Let's try using trial and error:

$$15 \times 1 \equiv 15 \pmod{26}$$
$$15 \times 2 \equiv 30 \equiv 4 \pmod{26}$$
$$15 \times 3 \equiv 45 \equiv 19 \pmod{26}$$
$$15 \times 4 \equiv 60 \equiv 8 \pmod{26}$$
$$15 \times 5 \equiv 75 \equiv 23 \pmod{26}$$
$$15 \times 6 \equiv 90 \equiv 12 \pmod{26}$$
$$15 \times 7 \equiv 105 \equiv 1 \pmod{26}$$

So, we found that $15 \times 7 \equiv 1 \pmod{26}$.

Therefore, the multiplicative inverse of 15 modulo 26 is 7.

Example: find the multiplicative Invers of 19 mod 26

26 = 19 * 1 + 7
19 = 7 * 2 + 5
7 = 5 * 1 + 2
5 = 2 * 2 + 1
2 = 2 * 1 + 0

Now, do the "backward part" of the algorithm 1 = 5 - 2*2

1 = 5 - 2(7 - 5*1)
1 = 5*3 - 2*7
1 = (19 - 7*2)*3 - 2*7
1 = 3*19 - 8*7
1 = 3*19 - 8(26 - 19*1)
1 = 11*19 - 8*26
1 = 11*19 mod 26

So, we conclude that 11 is the multiplicative inverse of 19 modulo 26.

Inverse

To find $11^7 \bmod 13$, we can proceed as follows:

$$11^2 = 121 \equiv 4 \pmod{13}$$
$$11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$$
$$11^7 = 11 \times 11^2 \times 11^4$$
$$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 \pmod{13}$$

$X = a^{p-2} \bmod p$ P must be Prime

$15^{-1} \bmod 17 = 8$ 17 must be Prime

$15^{17-2} \bmod 17$

$15^{15} \bmod 17$

$15^5 * 15^5 * 15^5 \bmod 17$

$15^5 = 759375 \bmod 17 = 2$

$2 * 2 * 2 = 8$

Sul2:

$15^{-1} \bmod 17 = 8$

17+17=34+1 / 15=2.3

34+17=51+1 / 15=3.4

51+17=68+1 / 15=4.6

68+17=85+1 / 15= 5.7

85+17=102+1 / 15=6.86

102+17=119+1 / 15= 8

Example: Using the extended Euclidean algorithm, find the multiplicative inverse of 7465 mod 2464

gcd(40902, 24240) = 34 ≠ 1, so there is no multiplicative inverse.