Home Inversion Calculator

Inverting Modulo

Parker McKillop, Oksana Pooley, Arsh Singh

Number
15

Modulo
26

Calculate

Resources

Euclidean Algorithm Modular Multiplicative Inverse

First Part: Euclidean Algorithm

Iter 1:

1

```
    ---
15 | 26
    -15
    ---
     11
```

Iter 2:

```
     1
    ---
11 | 15
    -11
    ---
     4
```

Iter 3:

```
     2
    ---
 4 | 11
    - 8
    ---
     3
```

Iter 4:

```
             1
            --
         3 | 4
            -3
            --
             1
```

Thus, GCD(15, 26) = 1

Euclidean algorithm gives us the following equations.

26 = 15 * 1 + 11 ... (1)

15 = 11 * 1 + 4 ... (2)

11 = 4 * 2 + 3 ... (3)

 4 = 3 * 1 + 1 ... (4)

Second Part: Reversing

Isolating 1 from (4)

1 = 4 * 1 + 3 * -1 ... (5)

Isolating 3 from (3) and putting in (5).

Rearrange to keep as a linear combination of 11 and 4:

1 = 11 * -1 + 4 * 3 ... (6)

Isolating 4 from (2) and putting in (6).

Rearrange to keep as a linear combination of 15 and 11:

1 = 15 * 3 + 11 * -4 ... (7)

Isolating 11 from (1) and putting in (7).

Rearrange to keep as a linear combination of 26 and 15:

1 = 26 * -4 + 15 * 7 ... (8)

Bézout's coefficients are -4 and 7.

The multiplicative inverse of 15 mod 26 is 7.
