2 Feb

02 February 2022 21:03

Modular Multiplication Inv.

a = 10 , m = 17

((a x n) % m == 1)

(7 x 5) % 5 == 0

(7 x 1) % 5 = 2 — 5

(7 x 2) % 5 = 4

(7 x 3) % 5 = 1

a = 5 m 7

5 x 1 % 7 = 5

5 x 2 % 7 = 3

5 x 3 % 7 = 1

5 x 4 % 7 = 6

5 x 7 % 7 = 0

5 x 8 % 7 = 5

5 x 9 % 7 = 3

5 x 10 % 7 = 1

5 x 11 % 7 = 6

a=3 m=2

```
mod MultInv( a, m ){
  for (i=1 to m-1){
   if ((a x i) % m == 1)
       return i;
  }
}
return -1;
}
```

SPrime

n = 20

[F, F, T, T, T, T, T, T, T, T, T, T, T, T, T, T, T, T, T, T]

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20

n=20

2 0

2

4

5

10

30

2

3

5

6

10

15

1	11
2	~~12~~
3	13
~~4~~	~~14~~
5	15
~~6~~	~~16~~
~~7~~	17
~~8~~	~~18~~
~~9~~	19
~~10~~	~~20~~

<- n/2 ->

j = SPrime ✓

x factor = not SPrime ✓

n/2 to n

n-1

$\frac{7}{2} = 3$

$i = \left(\frac{n}{2} + 1\right)$

n/2 to n

```
sprime(n) {
    count = 0
    for (i = (n/2)+1 to n) {
        if (isprime(i)) {
            count++;
        }
    }
    return count;
}
```

$\leq \sqrt{n}$

n = 50

2 to n

2 4 6 8 10 12 14 16 ....

3 6 9 12 15 ....

×4

5 25 35

6

7 49