

Modular Multiplication Inv.

$$a=10, m=17$$

$$(a \times n) \% m = \pm 1$$

$$(7 \times 5) \% 5 = 0$$

$$(7 \times 1) \% 5 = 2$$

$$(7 \times 2) \% 5 = 4$$

$$(7 \times 3) \% 5 = 1$$

$$a=5, m=7$$

$$5 \times 1 \% 7 = 5$$

$$5 \times 2 \% 7 = 3$$

$$5 \times 3 \% 7 = 1$$

$$5 \times 4 \% 7 = 6$$

$$5 \times 5 \% 7 = 2$$

$$5 \times 6 \% 7 = 4$$

$$5 \times 7 \% 7 = 0$$

$$5 \times 8 \% 7 = 5$$

$$5 \times 9 \% 7 = 3$$

$$5 \times 10 \% 7 = 1$$

$$5 \times 11 \% 7 = 6$$

$$a=3, m=2$$

mod MultInv(a, m) {

for (i=1 to m-1) {

if ((a * i) % m == 1)

return i;

}

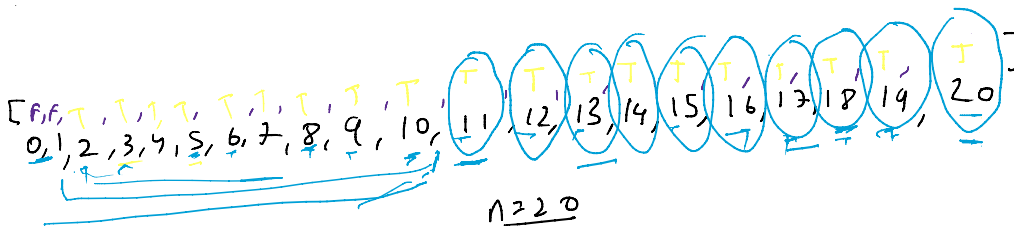
}

return -1;

}

S Prime

$$n=20$$



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

$$x \leftarrow \frac{n}{2}$$

$$i = \text{S Prime} \checkmark$$

$$x \text{ factor} = \text{not S prime} \checkmark$$

$$n/2 \text{ to } n$$

$$\frac{n-1}{2}$$



~~2~~ ~~3~~ (4) (5) (6) (7)

$n/2$ to n

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

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

isPrime(n) {

count = 0

for ($i = (n/2) + 1$ to n) {

if (isPrime(i)) {

count++;

}

return count;

}

$$\leq \sqrt{n}$$

$$n = 50$$

2 to n

<u>2</u>	4	6	8	10	12	14	16	...
<u>3</u>	6	9	12	15
<u>4</u>								
<u>5</u>	25	35						
<u>6</u>								
<u>7</u>	49							