**Homework for Section#2 (Approximate due date Aug 31st , 2020)**

1. Pick one prime number ***p*** greater than 5
   1. Generate the multiplication tables mod ***p***

**Prime Number (p): 13**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **13** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 2 | 2 | 4 | 6 | 8 | 10 | 12 | 1 | 3 | 5 | 7 | 9 | 11 |
| 3 | 3 | 6 | 9 | 12 | 2 | 5 | 8 | 11 | 1 | 4 | 7 | 10 |
| 4 | 4 | 8 | 12 | 3 | 7 | 11 | 2 | 6 | 10 | 1 | 5 | 9 |
| 5 | 5 | 10 | 2 | 7 | 12 | 4 | 9 | 1 | 6 | 11 | 3 | 8 |
| 6 | 6 | 12 | 5 | 11 | 4 | 10 | 3 | 9 | 2 | 8 | 1 | 7 |
| 7 | 7 | 1 | 8 | 2 | 9 | 3 | 10 | 4 | 11 | 5 | 12 | 6 |
| 8 | 8 | 3 | 11 | 6 | 1 | 9 | 4 | 12 | 7 | 2 | 10 | 5 |
| 9 | 9 | 5 | 1 | 10 | 6 | 2 | 11 | 7 | 3 | 12 | 8 | 4 |
| 10 | 10 | 7 | 4 | 1 | 11 | 8 | 5 | 2 | 12 | 9 | 6 | 3 |
| 11 | 11 | 9 | 7 | 5 | 3 | 1 | 12 | 10 | 8 | 6 | 4 | 2 |
| 12 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

* 1. Find the inverses mod ***p*** for all numbers k ∈ :{1, 2, …, p-1}

|  |  |
| --- | --- |
| **N** | **INV** |
| 1 | 1 |
| 2 | 7 |
| 3 | 9 |
| 4 | 10 |
| 5 | 8 |
| 6 | 11 |
| 7 | 2 |
| 8 | 5 |
| 9 | 3 |
| 10 | 4 |
| 11 | 6 |
| 12 | 12 |

* 1. Validate Fermat: (using arithmetic of 2.1)

if p = 17 then, 5p-1 = 512

512 1 mod 13

512  52 x 52 x 52 x 52 x 52 x 52 mod 13

(-1) x (-1) x (-1) x (-1) x (-1) x (-1) mod 13

1 mod 13

* 1. Validate Wilson: (p-1)!

(12)!

(12)! 12 x 10 x 9 x 8 x 7 x 6 x 5 x 4 x 3 x 2 x 1 mod 13

(22 x 31) x 11 x (51 x 21) x (32)x (23) x (71) x (31 x 21) x (51) x (22) x (31) x (21) mod 13

210 x 35 x 52 x 11 x 7 mod 13

210 x 35 x 52 x 12 mod 13

212 x 36 x 52 mod 13

24 x 24 x 24 x 36 x 52 mod 13

3 x 3 x 3 x 36 x 52 mod 13

33 x 33 x 33 x 52 mod 13

1 x 1 x 1 x (-1) mod 13

-1 mod 13

Hence, it is correct.

* 1. Check that

(13!) / (5! x 8!)

(13!) / (5! x 8!)

13 x 12! / (5! x 8!) mod 13

(13 x -1) / (5! x 8!) mod 13 (12! Mod 13 = 0, from previous question)

(13 x -1) / ((5 x 23 x 3) x (27 x 7 x 32 x 5)) mod 13

(13 x -1) / (52 x 210 x 33 x 7) mod 13

(13 x -1 x 82 x 710 x 93 x 2) mod 13

(13 x -1 x 27 x 39 x 710) mod 13

(13 x -1 x 3 x 23 x 13 x (-3)5) mod 13

(13 x -1 x 36 x 23 x -1) mod 13

(13 x -1 x 1 x 1 x -1 x 8) mod 13

(13 x 8) mod 13

(0 x 8) mod 13

0 mod 13

Hence, it is correct.

**Homework for Section#2 (Approximate due date Aug 31st , 2020)**

1. Compute the Euler parameter
   1. Generate the multiplication tables mod 3***p***

Taking p = 7

So, 3p = 21

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **21** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 2 | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 |
| 3 | 3 | 6 | 9 | 12 | 15 | 18 | 0 | 3 | 6 | 9 | 12 | 15 | 18 | 0 | 3 | 6 | 9 | 12 | 15 | 18 |
| 4 | 4 | 8 | 12 | 16 | 20 | 3 | 7 | 11 | 15 | 19 | 2 | 6 | 10 | 14 | 18 | 1 | 5 | 9 | 13 | 17 |
| 5 | 5 | 10 | 15 | 20 | 4 | 9 | 14 | 19 | 3 | 8 | 13 | 18 | 2 | 7 | 12 | 17 | 1 | 6 | 11 | 16 |
| 6 | 6 | 12 | 18 | 3 | 9 | 15 | 0 | 6 | 12 | 18 | 3 | 9 | 15 | 0 | 6 | 12 | 18 | 3 | 9 | 15 |
| 7 | 7 | 14 | 0 | 7 | 14 | 0 | 7 | 14 | 0 | 7 | 14 | 0 | 7 | 14 | 0 | 7 | 14 | 0 | 7 | 14 |
| 8 | 8 | 16 | 3 | 11 | 19 | 6 | 14 | 1 | 9 | 17 | 4 | 12 | 20 | 7 | 15 | 2 | 10 | 18 | 5 | 13 |
| 9 | 9 | 18 | 6 | 15 | 3 | 12 | 0 | 9 | 18 | 6 | 15 | 3 | 12 | 0 | 9 | 18 | 6 | 15 | 3 | 12 |
| 10 | 10 | 20 | 9 | 19 | 8 | 18 | 7 | 17 | 6 | 16 | 5 | 15 | 4 | 14 | 3 | 13 | 2 | 12 | 1 | 11 |
| 11 | 11 | 1 | 12 | 2 | 13 | 3 | 14 | 4 | 15 | 5 | 16 | 6 | 17 | 7 | 18 | 8 | 19 | 9 | 20 | 10 |
| 12 | 12 | 3 | 15 | 6 | 18 | 9 | 0 | 12 | 3 | 15 | 6 | 18 | 9 | 0 | 12 | 3 | 15 | 6 | 18 | 9 |
| 13 | 13 | 5 | 18 | 10 | 2 | 15 | 7 | 20 | 12 | 4 | 17 | 9 | 1 | 14 | 6 | 19 | 11 | 3 | 16 | 8 |
| 14 | 14 | 7 | 0 | 14 | 7 | 0 | 14 | 7 | 0 | 14 | 7 | 0 | 14 | 7 | 0 | 14 | 7 | 0 | 14 | 7 |
| 15 | 15 | 9 | 3 | 18 | 12 | 6 | 0 | 15 | 9 | 3 | 18 | 12 | 6 | 0 | 15 | 9 | 3 | 18 | 12 | 6 |
| 16 | 16 | 11 | 6 | 1 | 17 | 12 | 7 | 2 | 18 | 13 | 8 | 3 | 19 | 14 | 9 | 4 | 20 | 15 | 10 | 5 |
| 17 | 17 | 13 | 9 | 5 | 1 | 18 | 14 | 10 | 6 | 2 | 19 | 15 | 11 | 7 | 3 | 20 | 16 | 12 | 8 | 4 |
| 18 | 18 | 15 | 12 | 9 | 6 | 3 | 0 | 18 | 15 | 12 | 9 | 6 | 3 | 0 | 18 | 15 | 12 | 9 | 6 | 3 |
| 19 | 19 | 17 | 15 | 13 | 11 | 9 | 7 | 5 | 3 | 1 | 20 | 18 | 16 | 14 | 12 | 10 | 8 | 6 | 4 | 2 |
| 20 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

* 1. Find the inverses all numbers k ∈ : {*, , …,* }

|  |  |
| --- | --- |
| **N** | **INV** |
| 1 | 1 |
| 2 | 11 |
| 4 | 16 |
| 5 | 17 |
| 8 | 8 |
| 10 | 19 |
| 11 | 2 |
| 13 | 13 |
| 16 | 4 |
| 17 | 5 |
| 19 | 10 |
| 20 | 20 |

* 1. Verify Euler:

Here, = 2 x 6 = 12

So,

1112 mod 21

112 x 112 x 112 x 112 x 112 x 112 mod 21

1 x 1 x 1 x 1 x 1 x 1 mod 21

1 mod 12

Hence, it is correct.

* 1. Check: (3p-1)!

(3p-1)! (21 - 1)! mod 21

20! mod 12

20 x 19 x 18 x 17 x 16 x 15 x 14 x 13 x 12 x 11 x 10 x 9 x 8 x 7 x 6 x 5 x 4 x 3 x 2 x 1 mod 21

(3 x 7) x 20 x 19 x 18 x 17 x 16 x 15 x 14 x 13 x 12 x 11 x 10 x 9 x 8 x 6 x 5 x 4 x 2 x 1 mod 21

21 x 20 x 19 x 18 x 17 x 16 x 15 x 14 x 13 x 12 x 11 x 10 x 9 x 8 x 6 x 5 x 4 x 2 x 1 mod 21

0 x 20 x 19 x 18 x 17 x 16 x 15 x 14 x 13 x 12 x 11 x 10 x 9 x 8 x 6 x 5 x 4 x 2 x 1 mod 21

0 mod 21

Hence, it is correct.

* 1. Check (3p-1)! – (p-1)! ≡ 1 mod 3p

Here, p = 7, 3p = 21

(3p-1)! – (p-1)! ≡ (21-1)! – (7-1)! mod 21

≡ 20! – 6! mod 21

≡ 0 – 6! mod 21

≡ -(6 x 5 x 4 x 3 x 2 x 1) mod 21

≡ -(3 x 2 x 5 x 2 x 2 x 3 x 2 x 1) mod 21

≡ -(32 x 24 x 5) mod 21

≡ -(45 x 24) mod 21

≡ -(3 x 24) mod 21

≡ -(6) mod 21

≡ 15 mod 21

Hence, it is incorrect.