a ^ x mod 29

9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 1 1 1: 18 24 19 9 14 28 27 25 21 13 23 5 10 3: 21 5 15 16 19 28 4 12 26 20 18 8 24 14 13 28 25 13 23 5 4: 20 22 4 16 6 24 7 28 25 13 23 20 13 25 9 16 22 23 28 24 7 6 1 5 20 13 5: 9 16 22 23 28 24 4 4 25 6: 4 24 28 23 22 16 9 5 1 6 13 20 4 24 28 7 20 24 23 16 25 7: 20 23 16 25 8: 3 24 18 28 21 23 9 14 25 26 10 23 9: 5 20 6 25 22 24 13 9 4 5 16 28 20 6 25 2 20 26 28 19 16 5 21 10: 8 22 17 25 18 6 15 4 11 23 27 11: 22 10 23 21 28 18 15 20 16 24 17 13 27 12: 12 1 12 28 1 12 28 17 1 28 1 12 28 12 28 17 16 4 23 13: 20 28 5 7 9 13 24 22 25 20 28 6 5 28 25 2 14: 14 22 18 20 19 5 12 23 3 13 8 15 7 11 24 17 26 16 15: 23 26 13 21 25 28 18 17 14 19 25 23 16: 23 20 16 24 7 20 16 24 25 23 20 16 24 1 1 17 28 12 1 17 28 12 17: 17 28 12 1 17 28 12 1 17 28 12 1 17 28 12 17 16 27 22 19 23 8 28 11 24 26 18: 4 14 20 12 13 19: 11 6 27 20 3 28 10 16 14 5 8 18 23 20 23 25 1 20 23 25 20: 20 23 25 7 24 16 7 24 16 20 23 25 21: 4 26 24 11 28 8 6 10 2 13 12 20 14 23 19 22: 24 6 16 4 22 20 23 13 25 23: 7 16 23 20 25 24 23 7 16 24 23 20 25 24 16 20 25 24: 7 23 24 25 20 16 7 23 1 24 25 20 7 23 1 24 25 20 16 16 25: 16 23 24 20 1 25 16 23 24 20 28 26: 17 7 8 5 3 12 22 21 24 15 13 19 26 2 23 18 14 16 10 20 27 6 11 25 2 25 27: 4 21 16 26 6 17 24 10 9 11 7 15 28 8 13 3 23 12 5 19 20 18 22 14 28: 1 28 1 28 1 28 1 28 1 28 1 28 1 28 1 28 1 28 1 28 1 28

```
polynomial a ^{\circ} x mod x^{4} + x + 1 (0x13)
           3
               4
                  5
                     6
                       7
                           8
                              9 10 11 12 13 14 15
 1:
                     1
                        1
                           1
                              1
            1
 2:
         4 8 3 6 12 11
                           5 10
                                7 14 15 13
      3
         5 15 2
                  6 10 13
 3:
                           4 12
                                     9
                                        8
      4 3 12 5
                  7 15 9
                           2 8
 4:
                                  6 11 10 14 13
 5:
      5 2 10
              4
                  7 8 14
                           3 15 6 13 12
                                           9 11
                                       1
 6:
      6
           1
               6
                     1
                        6
                             1
                                           6
                                  6
                                     7
                                       1
                  6
                        7
                           6
 7:
         6
           1
                     1
                              1
                                     6
                                           7 6
 8:
      8 12 10 15
                  1
                     8 12 10 15
                                  1 8 12 10 15
        13 15 14
                                        8
 9:
                  7 10
                        5 11 12
                                     3
                                              2
                                           4
         8 15 12
                  1 10
                       8 15 12
                                  1 10
                                       8 15 12
10:
     10
         9 12 13
                          14
     11
                  6 15
                       3
                              8
                                     4
                                       10
11:
                                             5
12:
     12 15
            8 10
                  1 12 15
                           8 10
                                  1 12 15
                                           8 10 1
13:
                     8
     13 14 10 11
                  6
                        2
                            9
                             15
                                     5 12
                                           3 4 1
                          13 10
                  7 12
14:
     14 11
            8
                        4
                                     2 15
     15 10 12
               8
                  1 15 10
                          12
                                  1 15 10
15:
                             8
                                                 1
```