## Homework 1

Note: This homework is individual work!

1.What integers do the sets $Z_{38}$ and $Z_{38^*}$ contain? List all additive inverse pairs and multiplicative inverse pairs in the two sets.

$Z_{38}^* = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 21, 23, 25, 27, 29, 31, 33, 35, 37\}$

Multiplicative Inverse

$\{(1,1), (3,13), (5,23), (7,11), (9,17), (15,33), (21,29), (25,35), (27,31), (37,37)\}$

---

2. Using extended Euclidean algorithm, show the steps of finding the following multiplicative inverses

a) $323^{-1}$ mod 80979. 47384

b) $159^{-1}$ mod 56478 not exist

---

3. For the group $G = <Z_{32^*}, x>$

a. Find the order of the group

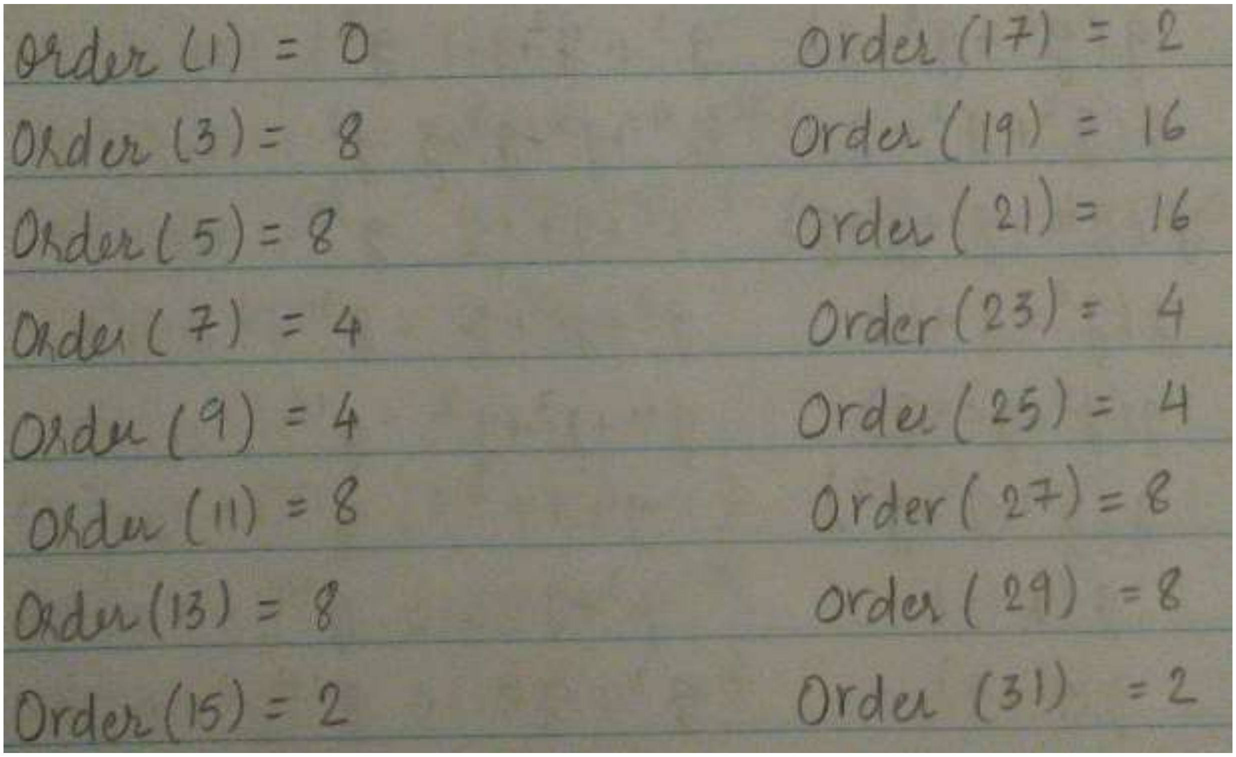
$Z_{32}^* = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\}$

$|G| = 16$

b. Find the order of each element in the group

Correction: ord(19) = order(21) = 8

Correction: ord(1) = 1



Order (1) = 0
Order (3) = 8
Order (5) = 8
Order (7) = 4
Order (9) = 4
Order (11) = 8
Order (13) = 8
Order (15) = 2
Order (17) = 2
Order (19) = 16
Order (21) = 16
Order (23) = 4
Order (25) = 4
Order (27) = 8
Order (29) = 8
Order (31) = 2

---

4. Using the irreducible polynomial $f(x) = x^5+x^4+x^3+x+1$ to

a) generate the elements of the field $GF(2^5)$

$x^5 = -x^4-x^3-x-1$

Since addition and subtraction are the same operation,

$x^5 = x^4+x^{3+}x+1$

| | | | | |
|---|---|---|---|---|
| $0 = 0$ | $= 0$ | $= 0$ | → | $0 =(00000)$ |
| $g^0 = g^0$ | $= g^0$ | $= g^0$ | → | $g^0 =(00001)$ |
| $g^1 = g^1$ | $= g^1$ | $= g^1$ | → | $g^1 = (00010)$ |
| $g^2 = g^2$ | $= g^2$ | $= g^2$ | → | $g^2 = (00100)$ |
| $g^3 = g^3$ | $= g^3$ | $= g^3$ | → | $g^3 = (01000)$ |
| $g^4 = g^4$ | $= g^4$ | $= g^4$ | → | $g^4 = (10000)$ |
| $g^5 = g^5$ | $= g^5$ | $= g^4 + g^3 + g+1$ | → | $g^5 = (11011)$ |
| $g^6 = g(g^5)$ | $= g(g^4 + g^3 + g+1)$ | $= g^3 + g^2 +1$ | → | $g^6 = (01101)$ |

| | | | | |
|---|---|---|---|---|
| $g^7 = g(g^6)$ | $= g(g^3 + g^2 + 1)$ | $= g^4 + g^3 + g$ | $\rightarrow$ | $g^7 = (11010)$ |
| $g^8 = g(g^7)$ | $= g(g^4 + g^3 + g)$ | $= g^3 + g^2 + g + 1$ | $\rightarrow$ | $g^8 = (01111)$ |
| $g^9 = g(g^8)$ | $= g(g^3 + g^2 + g + 1)$ | $= g^4 + g^3 + g^2 + g$ | $\rightarrow$ | $g^8 = (11110)$ |
| $g^{10} = g(g^9)$ | $= g(g^4 + g^3 + g^2 + g)$ | $= g^2 + g + 1$ | $\rightarrow$ | $g^{10} = (00111)$ |
| $g^{11} = g(g^{10})$ | $= g(g^2 + g + 1)$ | $= g^3 + g^2 + g$ | $\rightarrow$ | $g^{11} = (01110)$ |
| $g^{12} = g(g^{11})$ | $= g(g^3 + g^2 + g)$ | $= g^4 + g^3 + g^2$ | $\rightarrow$ | $g^{12} = (11100)$ |
| $g^{13} = g(g^{12})$ | $= g(g^4 + g^3 + g^2)$ | $= g + 1$ | $\rightarrow$ | $g^{13} = (00011)$ |
| $g^{14} = g(g^{13})$ | $= g(g + 1)$ | $= g^2 + g$ | $\rightarrow$ | $g^{14} = (00110)$ |
| $g^{15} = g(g^{14})$ | $= g(g^2 + g)$ | $= g^3 + g^2$ | $\rightarrow$ | $g^{15} = (01100)$ |
| $g^{16} = g(g^{15})$ | $= g(g^3 + g^2)$ | $= g^4 + g^3$ | $\rightarrow$ | $g^{16} = (11000)$ |
| $g^{17} = g(g^{16})$ | $= g(g^4 + g^3)$ | $= g^3 + g + 1$ | $\rightarrow$ | $g^{17} = (01011)$ |
| $g^{18} = g(g^{17})$ | $= g(g^3 + g + 1)$ | $= g^4 + g^2 + g$ | $\rightarrow$ | $g^{18} = (10110)$ |
| $g^{19} = g(g^{18})$ | $= g(g^4 + g^2 + g)$ | $= g^4 + g^2 + g + 1$ | $\rightarrow$ | $g^{19} = (10111)$ |
| $g^{20} = g(g^{19})$ | $= g(g^4 + g^2 + g + 1)$ | $= g^4 + g^2 + 1$ | $\rightarrow$ | $g^{20} = (10101)$ |
| $g^{21} = g(g^{20})$ | $= g(g^4 + g^2 + 1)$ | $= g^4 + 1$ | $\rightarrow$ | $g^{21} = (10001)$ |
| $g^{22} = g(g^{21})$ | $= g(g^4 + 1)$ | $= g^4 + g^3 + 1$ | $\rightarrow$ | $g^{22} = (11001)$ |
| $g^{23} = g(g^{22})$ | $= g(g^4 + g^3 + 1)$ | $= g^3 + 1$ | $\rightarrow$ | $g^{23} = (01001)$ |
| $g^{24} = g(g^{23})$ | $= g(g^3 + 1)$ | $= g^4 + g$ | $\rightarrow$ | $g^{24} = (10010)$ |
| $g^{25} = g(g^{24})$ | $= g(g^4 + g)$ | $= g^4 + g^3 + g^2 + g + 1$ | $\rightarrow$ | $g^{25} = (11111)$ |
| $g^{26} = g(g^{25})$ | $= g(g^4 + g^3 + g^2 + g + 1)$ | $= g^2 + 1$ | $\rightarrow$ | $g^{26} = (00101)$ |
| $g^{27} = g(g^{26})$ | $= g(g^2 + 1)$ | $= g^3 + g$ | $\rightarrow$ | $g^{27} = (01010)$ |
| $g^{28} = g(g^{27})$ | $= g(g^3 + g)$ | $= g^4 + g^2$ | $\rightarrow$ | $g^{28} = (10100)$ |
| $g^{29} = g(g^{28})$ | $= g(g^4 + g^2)$ | $= g^4 + g + 1$ | $\rightarrow$ | $g^{29} = (10011)$ |
| $g^{30} = g(g^{29})$ | $= g(g^4 + g + 1)$ | $= g^4 + g^3 + g^2 + 1$ | $\rightarrow$ | $g^{30} = (11101)$ |

b) **based on the results of a)**, calculate the followings in $GF(2^5)$

b.1) $(x^2 + x + 1)^{-1}$

$x^2 + x + 1 = g^{10}$

$(x^2 + x + 1)^{-1} = g^{-10 \bmod 31} = g^{21} = x^4 + 1$

b.2) $(x^3 - x + 1) \text{ X } (x^3 + x^2 + 1)$

$x^3 - x + 1 = x^3 + x + 1 = g^{17}$

$x^3 + x^2 + 1 = g^6$

$(x^3 - x + 1) \text{ X } (x^3 + x^2 + 1) = g^{17} \text{ x } g^6 = g^{23} = x^3 + 1$

b.3) $(x^4 - x + 1) / (x^3 + x + 1)$

$x^4 - x + 1 = x^4 + x + 1 = g^{29}$

$x^3 + x + 1 = g^{17}$

$(x^4 - x + 1) / (x^3 + x + 1) = g^{29-17} = g^{12} = x^4 + x^3 + x^2$

---

5. Find the results of following, using Fermat's little theorem or Euler's theorem.

| | |
|---|---|
| a) $26^{7039962} \bmod 59$ | 20 |
| b) $37^{-1} \bmod 416$ | 45 |
| c) $79^{-1} \bmod 398$ | 131 |
| d) $59^{-1} \bmod 676$ | 275 |
| e) $38^{433999802} \bmod 448$ | 128 |