Muhammad Izham Bin Norhamadi
B032020039
BITZ
S2G1

Tutorial 2: Introduction to Finite Field F_2

0. Let us take a number x =100+ (ID mod 100) and y = 200 +(MyKAD mod 100)

An addition is an exclusive-or operation

$x = 187$ and $y = 239$.

$x = 187_{10} = 1011\ 1011_2 = x^7 + x^5 + x^4 + x^3 + x + 1$ and

$y = 239_{10} = 1110\ 1111_2 = x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$,

$x + y = 1011\ 1011_2 + 1110\ 1111_2 =$

```
1110 1111
1011 1011
---------
0101 0100
```

In mathematical notation $x + y = (x^7 + x^5 + x^4 + x^3 + x + 1) + (x^7 + x^6 + x^5 + x^3 + x^2 + x + 1)$

$= 2x^7 + x^6 + 2x^5 + x^4 + 2x^3 + x^2 + x + 2$

$= 0x^7 + x^6 + 0x^5 + x^4 + 0x^3 + x^2 + x + 0 \pmod 2$

$= x^6 + x^4 + x^2 + x$

1. Multiplication is a convolution modulo 2.

$x \cdot y =$ $11101111_2 \cdot 10111011_2$

```
=11101111
   11101111
    11101111
     11101111
       11101111
        11101111
=110001011011001
```

2. Division gives quotient and remainder.

Let us divide by $283_{10} = 100011011_2 = x^8 + x^4 + x^3 + x + 1$

```
Quotient        110001011011001 = 25,305₁₀
     1          100011011
                ---------
                 10010000011001
     11          100011011
                 ---------
                  0011101111001
     11001          100011011
                    ---------
                     1100010101
     110011          100011011
                     ---------
                      100100011
     1100111          100011011
                      ---------
                       00111000 = 56₁₀ Reminder
```

3. An inverse is a good starting point to be a cryptographer.

Lets compute an inverse $x^5+x^4+x^3$ from previous number modulo $x^8 + x^4 + x^3 + x + 1$

Let us invoke an Extended Euclidean Algorithm

Extended Euclidean Algorithm

i	$b =$	a *	q	+	r	u	v	$w=u-vq$
0	100011011	111000	1101		11	0	1	1101
1	111000	11	10111		1	1	1101	11110011

```
Line 0: Quotient     100011011              w=u–vq =0-1·1101=1101
          1000       111000
                      11011011
          1100        111000
                       0111011
          1101          111000
                        000011 Remainder

Line 1: Quotient     111000                 w=u–vq =1-1101·10111
          10000      11                            =10111
                      01000                          10111
          10100        11                              10111
                        100                        11110011
          10110         11
                         10
          10111          11
                          1  Remainder
```

Line 0: $v \cdot q = 1 \cdot 1101 = 1 \cdot (x^3 + x^2 + 1) =$ 1101

Always remember to check your answer whether $a \cdot a^{-1} \equiv 1 \pmod{p}$

4. Check your division: Another say another A.

Let us check that

$a^{-1} = $ `11110011` is indeed an inverse of $a = $ `111000` modulo `100011011`.

$a \cdot a^{-1}$

```
= 111000 * 11110011
  11110011
   11110011
    11110011
= 1011011001
  100011011
   011101111
```