Lecture 2a: A Ring on Irreducible Polynomials

LEARNING OUTCOME
By the end of the lesson the student will be able to:

a) understand a concept of irreducible polynomial
b) compute a greatest common divisor between two polynomials via Euclidean algorithm
c) compute an inverse of polynomial a modulo irreducible polynomial b via an extended Euclidean algorithm.

A prime number is divisible by another positive integer. It cannot be factored into more than one integers greater than 1.
The prime number list is 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, … and so on.
Let us see a polynomial over finite field modulo 2, F_2.
Let us take a number,

$P(x) = a_n \cdot x^n + \ldots + a_2x^2 + a_1x^1 + a_0x^0$ written in little endian.

A mathematical programmer will see the number in terms of big endian.
$P(x) = a_0x^0 + a_1x^1 + a_2x^2 + \ldots + a_n \cdot x^n$ in an array $[a_0, a_1, a_2, \ldots, a_n]$.

An index number system(ins):
Let us take a number, $A = 8475_{10} = 8 \cdot 10^3 + 4 \cdot 10^2 + 7 \cdot 10^1 + 5 \cdot 10^0$ = `[8 4 7 5].`
$B = 9362_{10} = 9 \cdot 10^3 + 3 \cdot 10^2 + 6 \cdot 10^1 + 2 \cdot 10^0$ = `[9 3 6 2].`
Let us add $A + B = 17 \cdot 10^3 + 7 \cdot 10^2 + 13 \cdot 10^1 + 7 \cdot 10^0$ = `[17 7 13 7].`
$= 1 \cdot 10^4 + 7 \cdot 10^3 + 8 \cdot 10^2 + 3 \cdot 10^1 + 7 \cdot 10^0$ = `[1 7 8 3 7].`

This is called a carry problem. It is an inefficient process. Starting from 1980's, a polynomial in finite field has been introduced in cryptography.

A finite field F_2 is an n-bit polynomial
$P(x) = a_{n-1} \cdot x^{n-1} + \ldots + a_2x^2 + a_1x^1 + a_0x^0 = [a_{n-1}, \ldots, a_2, a_1, a_0]$ written in little endian modulo 2.

i	Binary	Polynomial
0	0	0
1	1	1
2	10	x
3	11	$x+1$
4	100	x^2
5	101	x^2+1
6	110	x^2+x
7	111	x^2+x+1
8	1000	x^3
9	1001	x^3+1
10	1010	x^3+x
11	1011	x^3+x+1
12	1100	x^3+x^2

Let us take a number, $A = 299_{10}$ $= [100101011] = x^8 + x^5 + x^3 + x + 1.$

$B = 283_{10}$ $= [100011011] = x^8 + x^4 + x^3 + x + 1.$

Let us add $A + B =$ $= [200112022] = 2x^8 + x^5 + x^4 + 2x^3 + 2x + 2.$

$= [\quad 110000] = x^5 + x^4 \pmod 2$

Similarly, an irreducible polynomial cannot be factored into the product of two polynomials. The property of irreducibility depends on the field or ring to which the coefficients are considered to belong.

A ring is a group with operations addition and multiplication. There must be also an identity for each operation. Traditionally, an identity for addition is a point zero. And an identity for multiplication is one.

Let x be a member of ring F_2, $x \in F_2$. An additive identity $e \in F_2$ so that

$$e + x = x + e = x.$$

An multiplicative identity $i \in F_2$ so that $i * x = x * i = x$. A good counter example we have seen in ECC, the identity is a point at infinity $(+\infty, +\infty)$.

Then there is an additive inverse $(-x) + x = x + (-x) = e$. And there is a multiplicative inverse

$$x^{-1} \cdot x = x \cdot x^{-1} = i.$$

A ring modulo irreducible polynomial over an integer has been practically popular since 1985. It has been used in several modern cryptosystems,

1. ECC (1985), 2. AES(2000), and 3. NTRU(2005).

We are in F_2. Let us review $x^2 - 1 = (x+1)\cdot(x-1) \equiv x^2 + 1$ is not an irreducible polynomial.

Let us take another example $P(x) = x^4 + x^3 + x^2 + x + 1$. Let $Q(x) = x - 1$.

$$P(x) \cdot Q(x) = (x-1) \cdot (x^4 + x^3 + x^2 + x + 1) = x^5 - 1 \equiv x^5 + 1$$

Let us see $(x-1) \cdot (x^4 + x^3 + x^2 + x + 1) = x^5 + x^4 + x^3 + x^2 + x$

$$-(x^4 + x^3 + x^2 + x + 1)$$

$$= x^5 - 1 \text{ is not an irreducible polynomial.}$$

Today, a ring modulo irreducible polynomial over positive integer coefficients is useful when an addition operation is taken as an exclusive-or.

Now, let us see how to generate the irreducible polynomial.

Prime versus Irreducible Polynomial in F_2

i	Binary	Polynomial
0	0	0
1	1	1
2	10	x
3	11	$x+1$
4	100	x^2
5	101	x^2+1
6	110	x^2+x
7	111	x^2+x+1
8	1000	x^3
9	1001	x^3+1
10	1010	x^3+x
11	1011	x^3+x+1
12	1100	x^3+x^2
13	1101	x^3+x^2+1

In this case of 5, x^2+1 is divisible by $x+1$. Since $x^2+1=(x+1)(x-1)=(x+1)(x+1)$

A Ring in Finite Field

A ring consists of 2 operations, addition and multiplication.

The addition operation is exclusive-or.

$a(x) = x^3+x+1$ and $b(x) = x^2+x+1$

$a = 1011$ and $b = 111$

$a(x) + b(x) = x^3+x+1 + x^2+x+1 = x^3+x^2$

$a \oplus b =$ 1011+111 =1100

```
 111
1100
```

Let us see multiplication. In the future, you will see a concept convolution for multiplication. We want to set a multiplier on the left with smaller number of ones. On the right we will set a longer string with more ones. This abelian operation,

$a \otimes b$ = 1011⊗111

= 111⊗1011

= 1011

```
  1011
 1011
1011
```

= 112221 =110001= x^5+x^4+1.

Let us take an example from S-box AES.

Let an irreducible polynomial $m = 283_{10} = 256+16+8+2+1=100011011_2$
In polynomial term, this irreducible polynomial $m(x) = x^8+ x^4+ x^3+ x +1$.

Let review and take an element $a = 42 = 32+8+2 = 101010_2$, $a(x) = x^5+ x^3+ x$.
We want to compute $a^{-1}(x)$ mod $m(x)$.

Let us review on how to compute greatest common divisor(gcd) in integer division
We write and express $b = a \cdot q + r$.

Euclidean Algorithm			
$b =$	$a \cdot$	$q +$	r
283	42	6	31
42	31	1	11
31	11	2	9
11	9	1	2
9	2	4	1
2	1	2	0

The answer is g = gcd(42, 283) =1. When the gcd is 1, they are linearly independent.
42 and 283 are relatively prime or coprime. The element 42 is invertible modulo 283.
There is an inverse.

Let us see the Extended Euclidean Algorithm

Euclidean Algorithm				Extended		
$b =$	$a \cdot$	$q +$	r	u	v	$w=u-v \cdot q$
283	42	6	31	0	1	-6
42	31	1	11	1	-6	7
31	11	2	9	-6	7	-20
11	9	1	2	7	-20	27
9	2	4	1	-20	27	-128
2	1	2	0	27	-128	283

a^{-1} mod b = $-128 +283 = 155$.
We always check $a \cdot a^{-1} \equiv 1 \pmod{b}$

$$42 \cdot 155 = 6510 = 23 \cdot 283 + 1 \equiv 1 \pmod{283}$$

Let us go into another domain in finite field F_2.
Let $a(x)$ and $b(x)$ be the polynomials respectively. In binary, $a = 42 = 32+8+2 = 101010 = x^5+x^3+x$
And $b = 283 = 256 +16+8+2+1=100011011 = x^8+x^4+x^3+x+1$.

Line	An Extended Euclidean Algorithm						
0	$b =$	$a \cdot$	$q +$	r	u	v	$w=u-v\cdot q$
1	100011011	101010	1010	11111	0	1	1010
2	101010	11111					

```
Line 1:     100011011  quotient
            101010     1000
              1001011
              101010   1010
                11111
```

Let us go back to school:

$$
\begin{array}{r}
x^3+x \\
x^5+x^3+x\overline{)x^8+x^4+x^3+x+1} \\
x^8+x^6+x^4 \\
\hline
x^6+x^3+x+1 \\
x^6+x^4+x^2 \\
\hline
x^4+x^3+x^2+x+1
\end{array}
$$

Line	An Extended Euclidean Algorithm						
0	$b =$	$a \cdot$	$q +$	r	u	v	$w=u-v\cdot q$
1	100011011	101010	1010	11111	0	1	1010
2	101010	11111	11	1011	1	1010	11111
3	11111	1011	11	10	1010	11111	101011
4	1011	10	101	1	11111	101011	10011000

```
Line 2:    101010      quotient        vq = 11*1010     u-vq  =11110
           11111       10                 = 1010               1
            10100                          1010          =11111
            11111      11                  11110
             1011

Line 3:    11111       quotient        vq = 11111*11    u-vq  =100001
           1011        10                 11111              1010
            1001                           11111            101011
            1011       11                  100001
              10

Line 4:    1011        quotient        vq = 101011*101  u-vq  =10000111
           10          100                101011               11111
             11                            101011         =10011000
             10         101                10000111
              1
```

Let us check $a(x) \cdot a^{-1}(x) = 1 \bmod m(x)$

```
      101010*10011000
=     10011000
        10011000
          100110000
      1011011110000 mod 100011011
      100011011
        11101000000
        100011011
         1100101100
         100011011
          100011010
          100011011
                1
```

Yes, $a^{-1}(x) = x^7 + x^4 + x^3$ is in fact an inverse of $a(x) = x^5+x^3+x$. Now, let us continue with the S-box.
From the $a = 42_{10} = 101010_2 = 2A_{16}$,
then $a^{-1} = 152_{10} = 10011000_2 = 98_{16}$.

This inverse will be plugged into an affine transform matrix.

One more time,

Let $a(x)$ and $b(x)$ be the polynomials respectively. In binary, $a = 43_{10} = 32+8+2+1 = 101011 = x^5+x^3+x+1$
And b = $283_{10} = 256 +16+8+2+1=100011011 = x^8+x^4+x^3+x+1$.

Line	Euclidean Algorithm						
0	b=	a*	q+	r	u	v	w = u–vq
1	100011011	101011	1010	10101	0	1	1010
2	101011	10101	10	1	1	1010	10101
3							
4							

Line 1:

```
1010            quotient
100011011
101011          1000
  1000011
  101011        1010
    10101
```

Line 2:

$w=u-vq = 1 - (x^3+x)\cdot x = 1 + (x^4 + x^2)$

```
                = 1-(1010)·10=1+10100
10
101011
10101
     1
```

The Extended Euclidean algorithm will stop when r reaches 1. The inverse is given by w.

We always check $a \cdot a^{-1} \equiv 1 \pmod{b}$

```
101011·10101=   101011
                  101011
                    101011
                1000110111 mod 100011011
                100011011
                         1
```

In AES algorithm, this irreducible polynomial is
$m(x) = x^8 + x^4 + x^3 + x + 1 = 100011011_2$ = or {01}{1B} in hexadecimal notation.
In the S-box of AES, take the multiplicative inverse in the finite field GF(2^8) first where element {00} is mapped to itself {00}.

Let us take $\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$ from the top left corner of the S-box and then

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = 01100011_2 = 63_{16}.$$

Note: A matrix multiplication here is written in big-endian.

One more time, Let us take $\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$ from the bottom right corner of the S-box and then we need to take multiplicative inverse first modulo the irreducible polynomial
$m(x) = x^8 + x^4 + x^3 + x + 1 = 100011011_2$

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = 10011100_2 = 9C_{16}.$$

An S-box used in the **SubBytes()** transformation is presented in hexadecimal index.

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Tutorial 3: An inverse of irreducible polynomial.
Take y = matrix ID mod 100 as the last 2 digit of ID number.

1. Take $a = 100 + y$, compute $a^{-1} \pmod{b}$
2. Convert a into a polynomial over F_2.
3. Take $a(x)$ as a polynomial, compute a^{-1} mod irreducible polynomial $b(x) = x^8 + x^4 + x^3 + x + 1$ where $b(2) = 283_{10}$.
4. Plug in an inverse into an Affine Transform to get an output for AES S-box.

An Affine Transform in AES is given as

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

a^{-1}	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	8D	F6	CB	52	7B	D1	E8	4F	29	C0	B0	E1	E5	C7
1	74	B4	AA	4B	99	2B	60	5F	58	3F	FD	CC	FF	40	EE	B2
2	3A	6E	5A	F1	55	4D	A8	C9	C1	0A	98	15	30	44	A2	C2
3	2C	45	92	6C	F3	39	66	42	F2	35	20	6F	77	BB	59	19
4	1D	FE	37	67	2D	31	F5	69	A7	64	AB	13	54	25	E9	09
5	ED	5C	05	CA	4C	24	87	BF	18	3E	22	F0	51	EC	61	17
6	16	5E	AF	D3	49	A6	36	43	F4	47	91	DF	33	93	21	3B
7	79	B7	97	85	10	B5	BA	3C	B6	70	D0	06	A1	FA	81	82
8	83	7E	7F	80	96	73	BE	56	9B	9E	95	D9	F7	02	B9	A4
9	DE	6A	32	6D	D8	8A	84	72	2A	14	9F	88	F9	DC	89	9A
A	FB	7C	2E	C3	8F	B8	65	48	26	C8	12	4A	CE	E7	D2	62
B	0C	E0	1F	EF	11	75	78	71	A5	8E	76	3D	BD	BC	86	57
C	0B	28	2F	A3	DA	D4	E4	0F	A9	27	53	04	1B	FC	AC	E6
D	7A	07	AE	63	C5	DB	E2	EA	94	8B	C4	D5	9D	F8	90	6B
E	B1	0D	D6	EB	C6	0E	CF	AD	08	4E	D7	E3	5D	50	1E	B3
F	5B	23	38	34	68	46	03	8C	DD	9C	7D	A0	CD	1A	41	1C

Table 3.2 An inverse table $a(x)$ mod $m(x) = x^8+x^4+x^3+x+1$.

Let $a(x) = x^5+x^3+x$ and $m(x) = x^8+x^4+x^3+x+1$ be the polynomials respectively.
For $a = 42_{10} = 32+8+2 = 101010_2 = x^5+x^3+x = 2A_{16}$. Trace along row 2 and column A, an answer is 98_{16}.
From the $a = 42_{10} = 101010_2 = 2A_{16}$, then $a^{-1} = 152_{10} = 10011000_2 = 98_{16}$. Thus, $a^{-1}(x) = x^7+x^4+x^3$.

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = 11100101 = E5_{16}.$$

One more time, take $a = 43_{10} = 32+8+2+1 = 101011_2 = x^5+x^3+x+1 = 2B_{16}$. Trace along row 2 and column B, an answer is 15_{16}. From the $a = 43_{10} = 101011_2 = 2B_{16}$, then $a^{-1} = 10101_2 = 15_{16}$. Thus, $a^{-1}(x) = x^4+x^2+1$.

Let us take another example: Suppose $a = 200 = 128+64+8 = 11001000_2 = C8_{16}$.
Then from an inverse table, we will get $a^{-1} = A9_{16} = 10101001_2$

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = 11101000_2 = E8_{16}.$$