1

Jan 2, 2010

ART OF COMPUTER PROGRAMING

DONALD E. KNUTH

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, \ldots\}$$

$$x + 5 = 0$$

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$$

$$2x = 1$$

$$\times \quad \mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z}\}$$

$$x^2 = 2$$

$$\times \quad \mathbb{R} = \{ \quad \}$$

$$x^2 + 1 = 0$$

$$\times \quad \mathbb{C}_{\mathbb{R}[i]} = \{a + ib \mid i^2 = -1,\ a, b \in \mathbb{R}\}$$

RSA

$\mathbb{Z}_2 = \{0, 1\}$ $+_2, \cdot_2$

$+_2$	0	1
0	0	1
1	1	0

$\cdot_2$	0	1
0	0	0
1	0	1

$\mathbb{Z}_3 = \{0, 1, 2\}$ $+_3, \cdot_3$

$+_3$	0	1	2
0	$\boxed{0}$	1	2
1	1	2	$\boxed{0}$
2	2	$\boxed{0}$	1

$\cdot_3$	0	1	2
0	0	0	0
1	0	$\boxed{1}$	2
2	0	2	$\boxed{1}$

$\mathbb{Z}_4 = \{0,1,2,3\}$ $+_4$, $\cdot_4$

$+_4$	0	1	2	3
0	$\boxed{0}$	1	2	3
1	1	2	3	$\boxed{0}$
2	2	3	$\boxed{0}$	1
3	3	$\boxed{0}$	1	2

$+_4$	0	1	2	3
0	0	0	0	0
1	0	$\boxed{1}$	2	3
2	0	2	0	2
3	0	3	2	$\boxed{1}$

$\mathbb{Z}_5 = \{0,1,2,3\_4\}$ $+_5$, $\cdot_5$

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$+_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$$\frac{2}{3} = ?$$

$$\frac{2}{3} = 2 \cdot 3^{-1} = 2 \cdot 2 = 4 \checkmark$$

$$\frac{1}{2} = 1 \cdot 2^{-1} = 1 \cdot 3 = 3 \checkmark$$

4

$\mathbb{Z}_n$ is a field $\Longleftrightarrow$ n is a prime no.

n	1	2	3	4	5	6	7	8	9
	×	✓	✓	?	✓	?	✓	?	?

$\mathbb{Z}_2 = \{0, 1\}$

$ax^2 + bx + c = 0$

$a \neq 0$

$a, b, c \in \mathbb{Z}_2$

✓ $x^2 + x + 1 = 0$

× $x^2 + x = 0$

× $x^2 + 1 = 0$

× $x^2 = 0$

Suppose $\alpha^2 + \alpha + 1 = 0$

$\mathbb{Z}_2[\alpha] = \{a + \alpha b \mid a, b \in \mathbb{Z}_2$
$\alpha^2 + \alpha + 1 = 0\}$

$\{0, 1, \underset{\alpha^2}{\underset{\shortparallel}{1+\alpha}}, \alpha\}$

$\alpha^3 = \alpha \cdot \alpha^2 = \alpha(1+\alpha) = \alpha + \alpha^2 = 1$

$GF(4) = \{0, 1, \alpha, \alpha^2\}$

$+$	0	1	α	α^2
0	$\boxed{0}$	1	α	α^2
1	1	$\boxed{0}$	α^2	α
α	α	α^2	$\boxed{0}$	1
α^2	α^2	α	1	$\boxed{0}$

$\times$	0	1	α	α^2
0	0	0	0	0
1	0	$\boxed{1}$	α	α^2
α	0	α	α^2	$\boxed{1}$
α^2	0	α^2	$\boxed{1}$	α

$GF(2^3) =$

$$ax^3 + bx^2 + cx + d = 0$$

$$a \neq 0, \quad a, b, c, d \in \mathbb{Z}_2$$

× $x^3 + x^2 + x + 1 = 0$

✓ $x^3 + x^2 + 1 = 0$

✓ $x^3 + x + 1 = 0$

× $x^3 + x = 0$

× $x^3 + x^2 = 0$

× $x^3 + 1 = 0$

× $x^3 = 0$

× $x^3 + x^2 + x = 0$

6

$GF(4) = \{0, 1, \alpha, \alpha^2\}$ Galois field

00 10 01 11 $a + \alpha b$

+	0	1	α	α^2
0	$\boxed{0}$	1	α	α^2
1	1	$\boxed{0}$	α^2	α
α	α	α^2	$\boxed{0}$	1
α^2	α^2	α	1	$\boxed{0}$

+	0	1	α	α^2
0	0	0	0	0
1	0	$\boxed{1}$	α	α^2
α	0	α	α^2	$\boxed{1}$
α^2	0	α^2	$\boxed{1}$	α

$$\alpha^3 + \alpha + 1 = 0$$

$$GF(8) = \{ a + \alpha b + \alpha^2 c \mid a, b, c \in \mathbb{Z}_2 \}$$

$$\{ 0, 1, \alpha, \alpha^2, \underset{\substack{\parallel \\ \alpha+1}}{\alpha^3}, \underset{\substack{\parallel \\ \alpha^2+\alpha}}{\alpha^4}, \alpha^5, \alpha^6 \}$$

$$\alpha^4 = \alpha^3 . \alpha = (\alpha+1).\alpha$$
$$= \alpha^2 + \alpha$$

$$\alpha^5 = \alpha^3 + \alpha^2 = 1 + \alpha + \alpha^2$$

$$\alpha^6 = \alpha + \alpha^2 + \alpha^3 = \alpha + \alpha^2 + \alpha + 1$$
$$= \alpha^2 + 1$$

$$\alpha^7 = \alpha(\alpha^2 + 1) = \alpha^3 + \alpha$$
$$= 1 + \alpha + \alpha = 1$$

$$
\begin{array}{ccc}
 & GF(2^m) & \\
 & \vdots & GF(p^m) \\
 & GF(2^4) & \vdots \\
 & | & \vdots \\
 & GF(2^3) & GF(p^3) \\
 & | & | \\
\mathbb{C} & GF(2^2) & GF(p^2) \\
| & | & | \\
\mathbb{R} & GF(2) = \mathbb{Z}_2 & \mathbb{Z}_p
\end{array}
$$

$$\alpha^4 = \alpha^2 + \alpha$$

$$\alpha^5 = \alpha^3 + \alpha^2 = \alpha + 1 + \alpha^2$$

$$\alpha^6 = \alpha^2 + \alpha + \alpha^3$$
$$= \alpha^2 + \alpha + \alpha + 1 = \alpha^2 + 1$$

$$\alpha^7 = \alpha(\alpha^2 + 1) = \alpha^3 + \alpha$$
$$= \alpha + 1 + \alpha = 1$$

$$\alpha^3 = \alpha + 1$$

$$(\alpha^3)^2 = (\alpha + 1)^2$$

$$\alpha^6 = \alpha^2 + 1$$

$$(a+b)^2 = a^2 + b^2$$

$$\boxed{\alpha^3 + \alpha^2 + 1 = 0}$$ ✓

$$\begin{array}{c} GF(3^2) \\ | \\ \mathbb{Z}_3 \end{array}$$