Section 1 :-

[1] Divisibility :

* b divides a : $b \mid a$

$$a = k \cdot b$$

k ↓ integer

* $a \mid b \wedge b \mid a \rightarrow a = \pm b$

* $b \neq 0 \longrightarrow b \mid 0$

* $a \mid b \wedge b \mid c \rightarrow a \mid c$

* $c \mid a \wedge c \mid b \rightarrow c \mid (ma + nb)$

Note

$a = k_1 b$
$b = k_2 a$
$a = k_1 k_2 a$
$1 = k_1 k_2$
∴ k_1, k_2 are int
∴ $k_1 = k_2 = \pm 1$

---

[2] Division algorithm

$$a = qn + r$$

$a \bmod n$

$$\frac{a}{n} = \left\lfloor \frac{a}{n} \right\rfloor + \frac{r}{n}$$

$\left\lfloor \frac{a}{n} \right\rfloor$ ↓ q

$0 \leq r < n$

[3] The Euclidean algorithm

* GCD

- $gcd(a,b) = gcd(a,-b) = gcd(-a,b) = gcd(-a,-b)$

- Two numbers are Relatively Primes if their gcd = 1

- $gcd(x,1) = 1$

- $gcd(x,0) = x$

- $gcd(a,b) = gcd(b, a \bmod b)$

EX 1 :

$gcd(60, 24)$

$60 = 2 \times 2 \times 3 \times 5$ (Prime factorization)
$24 = 2 \times 2 \times 2 \times 3$

$gcd = \underbrace{2 \times 2 \times 3}_{\text{Common}} = 12$

EX 2 :

$gcd(8, 15)$

$8 = 2 \times 2 \times 2$
$15 = 3 \times 5$

$gcd = 1$ (No Common Primes)

Ex 3: gcd(324, 266)

gcd(324, 266)

	q	r
324, 266	1	58
266, 58	4	34
58, 34	1	24
34, 24	1	10
24, 10	2	4
10, 4	2	2
4, 2	2	0

gcd

gcd(2, 0) = gcd(324, 266)

= 2

Note gcd(X, 0) = X

gcd(1973, 539)

	q	r
1973, 539	3	356
539, 356	1	183
356, 183	1	173
183, 173	1	10
173, 10	17	3
10, 3	3	1
3, 1		

gcd

gcd(3, 1) = gcd(1973, 539)

= 1

gcd(X, 1) = 1

Congruent modulo

- $a \equiv b \bmod n$

  $n \mid a-b$

- $a \equiv b \bmod n \longrightarrow b \equiv a \bmod n$
- $a \equiv b \bmod n \wedge b \equiv c \bmod n$

  $\longrightarrow a \equiv c \bmod n$

$(a+b) \bmod n = (a \bmod n + b \bmod n) \bmod n$

$(a-b) \bmod n = (a \bmod n - b \bmod n) \bmod n$

$(a * b) \bmod n = (a \bmod n * b \bmod n) \bmod n$

---

multiplicative inverse of 1759 mod 550

* اللي بالازرق دول دايما كدا

x	y	q	r
$a \leftarrow$ 1	$c \leftarrow$ 0	–	1759
$b \leftarrow$ 0	$d \leftarrow$ 1	$e \leftarrow$ 3	550
$a-be \leftarrow$ 1	$c-de \leftarrow$ -3	5	109
-5	16	21	5
106	-339	1	4
-111	355		(1)

$\left[\frac{1759}{550}\right]$ (3 → e)

109 → $1759 - \overset{e}{3} \times 550$

هتقف لما يكون صفر او واحد

** gcd = 1 لو ال [illegible] واحد → inverse = -111

صفر → ملوش inverse

Multiplicative inverse of 2414 mod 4092

x	y	q	r
1	0	-	2414
0	1	0	4092
1	0	1	2414
-1	0	1	1678
2	-1	2	736
-5	2	3	206
17	-7	1	136
-22	9	2	64
61	-25	9	8
-571	234	2	34 → gcd
1203	-493		0

inverse يعني

بما أن gcd = 1 يعني يوجد

gcd = 34 //

Polynomial Arithmatic

$f(x) = x^3 + x^2 + 2 \quad g(x) = x^2 - x + 1$

* $f(x) + g(x) = x^3 + 2x^2 - x + 3$
* $f(x) - g(x) = x^3 + x + 1$
* $f(x) \cdot g(x) = x^5 + 3x^2 - 2x + 2$
* $GF(2)$ Galios field of 2

Coefficients mod 2 field

$f(x) + g(x) = x^3 + x + 1$

$f(x) - g(x) = x^3 + x + 1$

$f(x) \cdot g(x) = x^5 + x^2.$

زي ما كنا بنكتب $a = qn + r$

بردوا نقدر نكتب ال Polynomial

$$f(x) = q(x)\,g(x) + r(x)$$

$$r(x) = f(x) \bmod g(x)$$

* لو $r(x) = 0$ يبقى $g(x) \mid f(x)$
* لو $g(x)$ مبتقسمش غير على ال 1 و نفسها يبقى اسمها irreducible (prime) Pol.

ازاي نجيب ال $q(x)$ و ال $r(x)$ ؟

Long Division

$f(x) = x^3 + x^2 + 2$

$g(x) = x^2 - x + 1$

$$
\begin{array}{r|l}
 & x + 2 \quad \leftarrow q(x) \\
\hline
x^2 - x + 1 & x^3 + x^2 + 2 \\
 & x^3 - x^2 + x \\
\hline
 & 2x^2 - x + 2 \\
 & 2x^2 - 2x + 2 \\
\hline
 & x \quad \leftarrow r(x)
\end{array}
$$

$q(x) = x + 2$

$r(x) = x$

$$GCD(x^6+x^5+x^4+x^3+x^2+x+1,\ x^4+x^2+x+1) \quad GF(2)$$

هنعمل زي ما كنا بنعمل مع الـ "" , قام بن هنحسب الـ $r(x)$ و $q(x)$ بالـ long division وفي كل خطوة هنعمل mod 2 عشان GF(2)

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

q	r
x^2+x	$+x^3+x^2+1$
$x+1$	0

وصلنا للصفر يبقى الـ GCD x^3+x^2+1

وبردوا لو وصلنا للواحد يبقى الـ

$$\begin{array}{r} x+1 \\ x^3+x^2+1 \;\big)\; x^4+x^2+x+1 \\ x^4+x^3+x \\ \hline x^3+x^2+1 \\ x^3+x^2+1 \\ \hline 0 \end{array}$$

(−) هتبقى (+) عشان mod 2

last non zero reminder

$GF(2^n)$ مبنعخش Powers الـ *
نأ كس الـ n

example

$f(x) = x^3 + x + 1$ $GF(2^4)$

$g(x) = x^3 + 1$ $m(x) = x^4 + x + 1$

$(f(x) * g(x)) \bmod m(x)$ عايزين نحسب

$(f(x) \cdot (x^3 + 1)) \bmod m(x)$

$(x^3 f(x) + f(x)) \bmod m(x)$

$[x^3 f(x) \bmod m(x) + f(x) \bmod m(x)] \bmod m(x)$

① $x^3 f(x) \bmod m(x)$

$x^6 + x^4 + x^3$ هنعمل بقسمة عادية

$$
\begin{array}{r|l}
 & x^2 + 1 \\
x^4 + x + 1 & x^6 + x^4 + x^3 \\
 & x^6 + x^3 + x^2 \\ \hline
 & x^4 + x^2 \\
 & x^4 + x + 1 \\ \hline
 & x^2 + x + 1
\end{array}
$$

② $f(x) \bmod m(x) = x^3 + x + 1$

long Div. هنعمل أول ما ال Power ال 4 هنحتاج

$(x^3 f(x) + f(x)) \bmod m(x)$

$= (x^2 + x + 1 + x^3 + x + 1) \bmod m(x)$

$= (x^3 + x^2) \bmod m(x)$

طريقة تانية

① $x^3 f(x) \bmod m(x)$

هنقسمها على خطوات

ⓐ $x f(x) = x^4 + x^2 + 1$ ($=4$)

$$\begin{array}{r} 1 \\ x^4+x+1 \,\big)\, x^4 + x^2 + 1 \\ \underline{x^4 + x + 1} \\ x^2 + 1 \end{array}$$

$x f(x) \bmod m(x) = x^2 + 1$

ⓑ $x^2 f(x) = x(x^2+1) = x^3 + x$

ⓒ $x^3 f(x) = x(x^3 + x) = x^4 + x^2$

$$\begin{array}{r} 1 \\ x^4+x+1 \,\big)\, x^4 + x^2 \\ \underline{x^4 + x + 1} \\ x^2 + x + 1 \end{array}$$

$x^3 f(x) \bmod m(x) = x^2 + x + 1$

ونكمل الباقي زي الطريقة الاولى

الطريقة الثانية

$x^3 \; x^2 \; x^1 \; x^0$

$f(X) = 1 \; 0 \; 1 \; 1$

$g(X) = 1 \; 0 \; 0 \; 1$

$m(X) = 1 \; 0 \; 0 \; 1 \; 1$

$m(X) - X^4 = 0 \; 0 \; 1 \; 1$

$x^3 f(X)$

Shift left by 1

(10) $x \cdot f(X)$: $1011 * 0010 = 10110$; $10110 \oplus 10011$ (Xor) $= 00101$

$x^2 \cdot f(X)$: $0101 * 0010 = 1010$

$x^3 \cdot f(X)$: $1010 * 0010 = 0100$; $0100 \oplus 0011 = 0111$

$x^3 \cdot f(X) = 0111 = x^2 + x + 1$

$x^3 * f(x) + f(x) = 0111 \wedge 1011$

$= 1100$

$= x^3 + x^2$