Padding:

Simple - 10^*

Multirate - $10^* \ldots 1$.

20/09/2022.

Divisibility:

* A nonzero b divides a if $a = mb$ for some m, where a, b and m are integers.

* b and divides a if there is no remainder on division.

* notation $b|a$ is commonly used to mean b divides a.

Prime numbers:

Numbers that are divisible by only 1 and by the number itself.

Relative prime numbers:

a and b are relative prime numbers if $\gcd(a,b) = 1$.

eg: 3 and 4.

Congruent mod:

$a \bmod n = b \bmod n$.

Eg: $73 \bmod 23 = 4 \bmod 23$.

Properties of divisibility:

* If $a|1$ then $a = \pm 1$
* If $a|b$ and $b|a$ then $a = \pm b$.
* Any $b \neq 0$ divides 0.
* If $a|b$ and $b|c$ then $a|c$.
* If $b|g$ and $b|h$ then $b|(mg+nh)$ for arbitrary integers m and n.

Division Algorithm:

Given any positive integer n and any nonnegative integer a, if we divide a by n

GCD:

GCD of a and b is the largest integer that divides both a and b.

$$\gcd(a,b) = \gcd(|a|, |b|).$$

i) gcd(72345, 43215).

ii) gcd(3486, 10292).

$72345 = 1 \times 43215 + 29130$

$43215 = 1 \times 29130 + 14085$

$29130 = 2 \times 14085 - 960$

$14085 = 14 \times 960 + 645$

$960 = 1 \times 645 + 315$

$645 = 2 \times 315 + 15$

$315 = 21 \times 15$

gcd(72345, 43215) = 15

iii) gcd(75, 32)

iv) gcd(117, 218).

$75 = 2 \times 32 + 11$

$32 = 2 \times 11 + 10$

$11 = 1 \times 10 + 1.$

$10 = 10 \times 1.$

gcd(75, 32) = 1

$218 = 1 \times 117 + 101$

$117 = 1 \times 101 + 16$

$101 = 6 \times 16 + 5$

$16 = 3 \times 5 + 1.$

$5 = 5 \times 1.$

gcd(117, 218) = 1.

Modular Arithmetic:

* Congruent modulo n:

Two integers a and b are said to be congruent modulo n if $(a \bmod n) = (b \bmod n)$

* Modulus:

If a is an integer and n is a positive integer we define $a \bmod n$ to be the remainder when a is divided by n the integer is called modulus.

Properties:

1. $a = b \pmod n$ if $n(a-b)$
2. $a = b \pmod n$ implies $b = a \pmod n$
3. $a = b \pmod n$ and $b = c \pmod n$ imply $a = c \pmod n$.

Let $a = 23$, $b = 8$, $n = 5$.

$23 = 8 \pmod 5$

$23 - 8 = 15 = 5 \times 3$.

$\Rightarrow -11 = 5 \pmod 8$

$-11 - 5 = -16 = -2 \times 8$,

$[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n.$

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

$[(a \bmod n) * (b \bmod n)] \bmod n = (a*b) \bmod n.$

Commutative laws

Associative laws

Distributive law

Identities

Additive Inverse law

Format's Theorem:

If p is prime and a is a positive integer not divisible by p then.

$$a^{p-1} = 1 \pmod{p}.$$

Alternative form is:

If p is a prime and a is a positive integer then

$$a^p = a \pmod{p}.$$

$5^{19-1} = 1 \pmod{19} = 1$

$5^{19} = 5 \pmod{19} = 5$

BL!

Datours using: dtors

Short writes table

Overwriting offset modes.

node search.

12/10/2022

Euler's theorem: $a^{\phi(n)} \bmod n = 1$.

$\phi(n) = n-1$ if n is a prime numb

$\phi(n) = (p-1)(q-1)$ if $n = pq$ where p and q are prime numbers.

$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$ if $n = ab$ where a and b or either of them is compo

$\phi(7000) =$

$7000 = 7 \times 1000$

$= 7^1 \times 2^3 \times 5^3$

$\therefore \phi(7000) = 7000\left(1-\frac{1}{7}\right)\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)$

$= 7 \times 4000\left(1-\frac{1}{7}\right) = 24000$

Using Euler theorem Solve:

$4^{99} \bmod 35$ $\quad \phi(35) = 24.$

$= 4^{96} \cdot 4^{3} \bmod 35$

$= (4^{24})^{4} \cdot 4^{3} \bmod 35.$

$= (1 \bmod 35)^{4} \cdot 4^{3} \bmod 35$

$= 1 \cdot 64 \bmod 35$

$= 29.$

$3^{202} \bmod 13.$ $\quad \phi(13) = 12.$

$= (3^{12})^{16} \cdot 3^{10} \bmod 13$

$= (1 \bmod 13)^{16} \cdot 3^{10} \bmod 13$

$= 3^{10} \bmod 13.$

$= 3^{3} \cdot 3^{3} \cdot 3^{3} \cdot 3^{1} \bmod 13.$

$= 27 \bmod 13 \quad 9 \times 9 \times 9 \times 3$

$= 3.$

Chinese remainder theorem:

Step 1: Identify or calculate $m_1, m_2, \ldots$

Step 2: $M = m_1 \times m_2 \times m_3 \times \ldots m_i$

Step 3: $M_i = \frac{M}{m_i}$

Step 4: Calculate $a_1, a_2 \ldots a_i$

Step 5: Calculate M_i^{-1}

Step 6: $x = \sum_i a_i m_i M_i^{-1}$

$x = a_i \bmod m_i$

$x = 2 \bmod 3$

$x = 3 \bmod 5$ Using CRT.

$x = 2 \bmod 7$

It is used when $m_i > n$ ($a_i^n \bmod m_i$)

Step 1: $m_1 = 3 \quad m_2 = 5 \quad m_3 = 7$

Step 2: $M = 3 \times 5 \times 7 = 105$

Step 3: $M_1 = \frac{105}{3} = 35 \quad M_2 = \frac{105}{5} = 21$

$M_3 = \frac{105}{7} = 15$

Step 4: $a_1 = 2, a_2 = 3, a_3 = 2$

Step 5: M_i^{-1}

$M_i M_i^{-1} = 1 \bmod m_i$.

$35 \times 1 \bmod 3 = 2$

$35 \times 2 \bmod 3 = 1$

$M_1^{-1} = 2$

$21 \times 1 \bmod 5 = 1$

$M_2^{-1} = 1$

$15 \times 1 \bmod 7 = 1$

$M_3^{-1} = 1$.

Step 6:

$X = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1$.

$= 120 + 15 + 14$.

$X = 233 \bmod 115 = 23$.

How:

1) $4X = 5 \bmod 9$

$2X = 6 \bmod 20$.

2) $X = 5 \bmod 3$

$X = 2 \bmod 5$

$X = 1 \bmod 11$.

17/10/22.

Miller Rabin Primality test :

$n-1 = 2^k * m$

$a \quad 1 \leq a \leq (n-1).$

$b_0 = a^m \bmod n.$

$b_1 = b_0^2 \bmod n$

$b_2 = b_1^2 \bmod n.$

1) 561 a P. number

i) $561 = (n-1) \Rightarrow 561-1 = 560 = 2^4 \times 35.$

ii) $a = 2$

iii) $b_0 = 2^{35} \bmod 561.$

$= 263. \neq \pm 1$

$b_1 = (263)^2 \bmod 561.$

$= 166 \neq \pm 1$

$b_2 = (166)^2 \bmod 561.$

$= 67 \neq \pm 1.$

$b_3 = (67)^2 \bmod 561.$

$= 1.$

Composite number.

2) 53 a Prime number?

i) $53 \Rightarrow (n-1) = 52 = 2^2 \times 13$.

Addictive inverse of 53 is -1.

∴ It is Prime number

G.F Galois Fuelpl of Prime number:

* order of finite field is given as p^n.
* used in polynomial prime
* used in AES.

GF(2) :

(0,1) : {+, ×, +3}

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

$*_2$	0	1
0	0	0
1	0	1

a	0	1
-a	0	1
a^{-1}	-	1

GF(5) :

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

a	-a	a^{-1}
0	0	-
1	4	1
2	3	3
3	2	2
4	1	4.

GF(7), GF(8).

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$*_7$	0	1	2	3	4	5	6.
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4.
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1.

a	-a	a^{-1}
0	0	-
1	7	1
2	6	-
3	5	3
4	4	-
5	3	5
6	2	-
7	1	7

26/10/22

Not every element have inverse so we move to polynomial. ($a_i x^i$)

maximum degree = n-1. (eg: 2^3 degree = 3)

Polynomial addition => Xor.

0 - 000 → 0
1 - 001 → 1
2 - 010 → x
⋮
7 - 111 → x^2+x+1.

$$\begin{array}{r} x^2+x+1 \\ x^2+1 \\ \hline 0+x+0 \end{array}$$

$= x$ (2).

Polynomial multiplication => multiply and th
Xor.

eg: x^2+x+1

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

$= x^4+x^3+x+1$

$m(x) = x^3 + x + 1.$

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

$m(x) = x^8 + x^4 + x^3 + x + 1$ for $GF(2^8)$.

(2)

$$
\begin{array}{r}
x + 1 \\
* \quad x^2 + x \\
\hline
x^3 + x^2 + x^2 + x \\
\underline{\quad\quad\quad} \\
x^3 + x.
\end{array}
$$

$$
\begin{array}{r|l}
 & 1 \\
\hline
x^3+x+1 & x^3 + x \\
 & x^3 + x + 1 \\
\hline
 & \boxed{1\,1}
\end{array}
$$

$f(x) = x^6 + x^4 + x^2 + x + 1$

$g(x) = x^7 + x + 1$

$m(x) = x^8 + x^4 + x^3 + x + 1$

$f(x) + g(x) = x^7 + x^6 + x^4 + x^2$

multiplication:

$$= x^{13} + x^7 + x^6 + x^{11} + x^5 + x^4 + x^9 + x^3 + x^2 + x^8 + x^2 + x + x^7 + x + 1.$$

$$= x^{13} + x^{11} + x^9 + x^6 + x^5 + x^4 + x^3 + 1$$

$x^5 + x^3 + 1$

$x^8 + x^4 + x^3 + x + 1$) $x^{13} + x^{11} + x^9 + x^6 + x^5 + x^4 + x^3 + 1$

$x^{13} + x^9 + x^8 + x^6 + x^5$

$x^{11} + x^8 + x^4 + x^3 + 1$

$x^{11} + x^7 + x^6 + x^4 + x^3$

$x^8 + x^7 + x^6 + 1$

$x^8 + x^4 + x^3 + x + 1$

$x^7 + x^6 + x^4 + x^3 + x$

Assignment:

Take one application apply any hashing function to get output. (eg. SHA-256)