Number Theory

Saturday, 30 November 2019 10:59 AM

① Euclid's algorithm:

$$\gcd(r_0, r_1) = \gcd(r_0 \bmod r_1, r_1) = \gcd(r_1, r_0 \bmod r_1)$$

② Extended Euclidean algorithm:

$$\underbrace{\gcd(r_0, r_1)}_{\text{by euclids algorithm}} = s\, r_0 + t\, r_1$$

Idea: compute regular EA $\xrightarrow{\text{how?}}$

$\gcd(r_0, r_1)$: $r_0 = q_1 r_1 + r_2$ $\quad r_2 = s_2 r_0 + t_2 r_1$

$\gcd(r_1, r_2)$: $r_1 = q_2 r_2 + r_3$ $\quad r_3 = s_3 r_0 + t_3 r_1$

⋮ ⋮ ⋮

$\gcd(r_{l-2}, r_{l-1})$: $r_{l-2} = q_{l-1} r_{l-1} + r_l$ $\quad r_l = s_l r_0 + t_l r_1 = \gcd(r_0, r_1)$

$r_{l-1} = q_l r_l + 0$

∴ s and t are s_l, t_l here. (b)

how?

eg: $\gcd(973, 301) = s \cdot 973 + t \cdot 301 = 7$

i

2 $\quad \underset{r_0}{973} = 3 \cdot \underset{r_1}{301} + \underset{r_2}{70}$

$r_2 = 70 = \boxed{[1]}\, 973 + \boxed{[-3]}\, 301$

3 $\quad 301 = 4 \cdot 70 + \overset{r_3}{21}$

$r_3 = 21 = 301 - 4 \; 70$ we need a multiple in terms of 973 & 301

soln → substitute from previous iteration

$r_3 = 21 = 301 - 4\,[973 - [3] \times 301]$

$r_3 = \boxed{[-4]}\, 973 + \boxed{[13]}\, 301$

4: $70 = 3 \cdot 21 + \overset{r_4}{7}$

$r_4 = 70 - 3 \cdot 21$ FROM 2 LINES (ITERATIONS BACK) FROM 1 LINE BACK

$7 = [1]\, 973 + [-3]\, 301 - 3\,[[-4]\, 973 + [13]\, 301]$

$7 = \boxed{[13]}\, 973 + \boxed{[-42]}\, 301$

in general:

$\boxed{r_{i-2}} = s_{i-2}\, r_0 + t_{i-2}\, r_1$

$\boxed{r_{i-1}} = s_{i-1}\, r_0 + t_{i-1}\, r_1$

next iteration:

EA: $r_{i-2} = q_{i-1}\, r_{i-1} + r_i$

$r_i = \boxed{r_{i-2}} - q_{i-1}\, \boxed{r_{i-1}}$

substitute back

$r_i = [s_{i-2} - q_{i-1}\, s_{i-1}]\, r_0 + (t_{i-2} - q_{i-1}\, t_{i-1}]\, r_1$

$r_i = s_i\, r_0 + t_i\, r_1$

Recursive Formulae

$s_i = s_{i-2} - q_{i-1}\, s_{i-1}, \quad i \geq 2$

$t_i = t_{i-2} - q_{i-1}\, t_{i-1}, \quad i \geq 2$

where $s_0 = 1 \quad t_0 = 0$

$s_1 = 0 \quad t_1 = 1$

MAIN APPLICATION OF EEA is COMPUTING OF INVERSES Mod n

problem: $a^{-1} \equiv ? \mod n$

$a^{-1} a \equiv 1 \mod n$ (by defn)

$\gcd(n, a) = 1$ [if $\exists\, a^{-1}$, then $\gcd(n,a)$ must be 1]

$= s \cdot n + t \cdot a$ (by EEA)

$1 = s \cdot n + t \cdot a$

take mod n both sides

$1 = s \cdot n + t \cdot a$

take mod n both sides

$1 \bmod n = (s \cdot n + t \cdot a) \bmod n$

$1 = 0 + t \cdot a \bmod n$

$\Rightarrow \quad ta \equiv 1 \bmod n$

$\therefore$ t is actually a^{-1}

↳ parameter of the smaller number

SOME THEOREMS:

(1) EULER'S PHI FUNCTION:

$\mathbb{Z}_m = \{0, 1, \ldots\ldots m-1\}$

$\gcd(0, m) = m$
$(1, m) =$
$(2, m) =$
$\vdots$
$(m-1, m) =$

how many are coprime to m?

eg: $m = 6$

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$\gcd(0, 6) = 6$
$(1, 6) = 1$ ✓
$(2, 6) = 2$
$(3, 6) = 3$
$(4, 6) = 2$
$(5, 6) = 1$ ✓

$\phi(6) = 2$

but this BRUTE FORCE is not viable for higher m.

sol^n:

$m = p_1^{e1} \cdot p_2^{e2} \cdot \ldots\ldots p_n^{en}$

$p_i \rightarrow$ distinct prime number

$e_i \rightarrow$ +ve integer

$\phi(m) = \prod_{i=2}^{m} (p_i^{e_i} - p_i^{e_i - 1})$

eg: $m = 240$

$\phi(240) = ?$

$m = 16 \cdot 15$
$= 2^4 \cdot 3^1 \cdot 5^1$

$$\phi(240) = \prod_{i=1}^{3} (p_i^{e_i} - p_i^{e_i - 1})$$

$$= (2^4 - 2^3)(3^1 - 3^0)(5^1 - 5^0)$$

$$= 8 \cdot 2 \cdot 4$$

$$= 64$$

(2) FERMATS LITTLE THEOREM

$a \to$ integer , $p \to$ prime

$$a^p \equiv a \pmod{p}$$

EULER'S THEOREM

$a, m \to$ integers s.t. $\gcd(a, m) = 1$

then :

$$a^{\phi(m)} \equiv 1 \pmod{m}$$