Date / /
Page No.

GCD

a = 20
b = 12

```
12 | 20 | 1
     12
   ----
    8 | 12 | 1
        8
      ----
      4 | 8 | 2
          8
        ----
        0 | 4 |
```

gcd (20, 12) = 4

gcd(a, b) = gcd(b, a%b)

gcd(a, 0) = a

```
int gcd (a, b) {
    if b == 0
        return a
    return gcd (a, b%a)
}
```

Time complexity of gcd

gcd (a, b) = gcd (a, b%a) $0 \le x \le b-1$

x

$x = a \% b = a - \left\lfloor \frac{a}{b} \right\rfloor b$ ... (1) floor

$x = a \% b \le a - b$ ... (2)

$x \le a - b$

$x \le b - 1$

$\Rightarrow 2x \le a - b + b - 1$

$2x \le a - 1$

$2x < a$

$x < \frac{a}{2}$

Date / /
Page No.

$$gcd(a,b) = gcd\left(b, \frac{a}{2}\right)$$

$$gcd\left(\frac{a}{2}, \frac{a \% b}{2}\right)$$

$$gcd(a,b) = \log_2(a)$$

Extended Euclid Algo

$Ax + By = GCD(A,B)$

$x, y = ?$

$GCD(A,B) = GCD(B, A\%B)$

$A\%B = A - \left[\frac{A}{B}\right]B$

$Ax + By = GCD(A,B)$

$Bx_1 + (A\%B)y_1 = GCD(B, A\%B)$

$\Rightarrow Bx_1 + \left[A - \left\{\frac{A}{B}\right]B\right] y_1 = GCD(A,B)$

$By + \sim A\, x$

$B\left[x_1 - \left[\frac{A}{B}\right]y_1\right] + Ay_1 = GCD(A,B)$ — (2)

$By + Ax = GCD(A,B)$

$$\boxed{\begin{aligned} x &= y_1 \\ y &= x_1 - \left[\frac{a}{b}\right]y_1 \end{aligned}}$$

→ Extended Euclid's Algorithm

Date / /
Page No.

A. = 18 , B = 30

$18x + 30y = \gcd(18, 30)$ (2, -1)

$30x_1 + 18y_1 = \gcd(30, 18)$ (-1, 2)

$18x_2 + 12y_2 = \gcd(18, 12)$ (1, -1)

$12x_3 + 6y_3 = \gcd(12, 6)$ (0, 1)

$6x_4 + 0y_4 = \gcd(6, 0)$ Base case (1, 0)

$6x_4 + 0 = 6$

$x_4 = 1, y_4 = 0$

$y = (-1 - (0)2)$

$y = \left[1 - \frac{30}{18}(-1)\right]$

$= 1 + 1 \to 2$

$y = \left[0 - \frac{18}{12}(1)\right]$

$y = \left[1 - \left(\frac{12}{6}\right)0\right] \to 1$

formula used

current $x = y$

current $y = \left[x - \left[\frac{a}{b}\right]y\right]$