정수론 9강 선형방정식의 해 (2)

$ax+by=g$의 선형방정식의 해.

$\Rightarrow \left(x_0 + k\cdot\frac{b}{g},\ y_0 - k\cdot\frac{a}{g}\right)$

* 이번시간
$ax+by=c$를 알아보자. $\gcd(a,b)=g$

i) $g \nmid c \Rightarrow ax+by$ 값의 꼴. $\Rightarrow$ 해가 없다.
$\hookrightarrow$ g의 배수.

$ax_0+by_0=g$ $\exists(x_0, y_0)$ (x_1, y_1)

$\boxed{ax+by}$ = g의 배수. $x_1 = x_0+\alpha,\ y_1 = y_0+\beta$

$\alpha, \beta = 0$

$ax_1+by_1 = a(x_0+\alpha)+b(y_0+\beta)$

$= ax_0 + a\alpha + by_0 + b\beta$

$= g + a\alpha + b\beta$

$g|a, g|b \Rightarrow g|a\alpha, g|b\beta \Rightarrow g|a\alpha+b\beta+g$

ii) $g|c$, $\frac{a}{g}u + \frac{b}{g}v = 1$ 가 되게 하는
확장된 유클리드 알고리즘
(u_0, v_0)가 있을까? $\gcd\left(\frac{a}{g}, \frac{b}{g}\right)=1$

$\Rightarrow ax+by=c$ 에서 $x_0 = \frac{c}{g}u_0,\ y_0 = \frac{c}{g}v_0$

$a\frac{c}{g}u_0 + b\cdot\frac{c}{g}v_0 = c\left(\frac{a}{g}u_0 + \frac{b}{g}v_0\right) = c$

(x_1, y_1)

$$\begin{array}{rl} & ax_0+by_0=c \\ - & ax_1+by_1=c \\ \hline & a(x_0-x_1)+b(y_0-y_1)=0 \end{array}$$

$\frac{a}{g}(x_0-x_1) = -\frac{b}{g}(y_0-y_1)$

$\frac{a}{g} | y_0-y_1 \Rightarrow$

$\frac{b}{g} | x_0-x_1 \Rightarrow$

$x_1 = x_0 + k\cdot\frac{b}{g}$

$y_1 = y_0 - k\cdot\frac{a}{g}$