$R = 7\mathbb{L}$

$r_0 \quad r_1 \quad q_1 \quad r_2$
$77 = 63 \cdot 1 + 14$
$r_1 \quad r_2 \quad q_2 \quad r_3$
$63 = 14 \cdot 4 + 7$
$r_2 \quad r_3 \quad q_3 \quad r_4$
$14 = 7 \cdot 2 + 0$

$\gcd(a,b) = 7$

$77 = 7 \cdot 11 \quad 63 = 7 \cdot 9$

$77 - 63 \cdot 1 = 14$
$63 \cdot 1 - 14 \cdot 4 = 7$
$63 \cdot 1 - (77 - 63) \cdot 4 = 7$

$77 \cdot \underbrace{(-4)}_{s} + 63 \cdot \underbrace{5}_{t} = \underbrace{7}_{\gcd}$


quotient
remainder

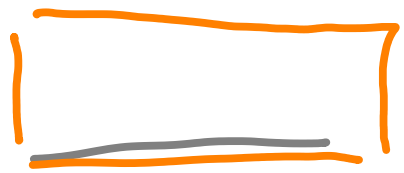
$$\mathbb{N} \cup \{-\infty\}$$

we have done ℓ divisions

$r_{i-1} - q_i r_i = r_{i+1}$ $\qquad$ $r_{i-2} = q_{i-1} r_{i-1} + r_i$

$r_{i-1} - q_i (r_{i-2} - q_{i-1} r_{i-1}) = r_{i+1}$

$r_0 \cdot s + r_1 \cdot t = r_2$



$r_0 = a$ $\qquad$ $r_1 = b$ $\qquad$ $\gcd(a,b) \mid r_0, r_1$

$\gcd(a,b) \mid r_0 - r_1 \cdot q_1 = r_2$

induction $\gcd(a,b) \mid r_i \quad \forall\, i \geq 0.$

$r_\ell \mid \gcd(a,b)$ $\qquad$ enough $r_\ell \mid a, b$

induction: $r_\ell \mid r_i$, $i \leq \ell$.

$r_\ell \mid r_{\ell-1}$ $\qquad$ $r_{\ell-2} = q_{\ell-1} \cdot r_{\ell-1} + r_\ell \Rightarrow r_\ell \mid r_{\ell-2}$

ℓ divisions with remainder

$$div(r_{i-1}, r_i) \longmapsto c \cdot \lg q_i \cdot \lg r_i$$

$$\boxed{\lg q_i = \lg r_{i-1} - \lg r_i}$$

$$div(r_{i-1}, r_i) \longmapsto c \cdot (\lg r_{i-1} - \lg r_i) \cdot \lg r_i$$

$$\sum_{i=1}^{\ell} \lg q_i = \sum_{i=1}^{\ell} (\lg(r_{i-1}) - \lg(r_i)) = \lg r_0 - \lg r_\ell \leq \lg r_0$$

$\lg r_1 > \lg r_2 > \cdots$

size function of Euclidean domain

total running time $\sum_{i=1}^{\ell} \operatorname{div}(r_{i-1}, r_i) =$

$= c \sum_{i=1}^{\ell} (\lg r_{i-1} - \lg r_i) \cdot \lg r_i$

$\lg r_i \leq \lg r_1$

$\leq c \cdot \lg r_1 \sum_{i=1}^{\ell} (\lg r_{i-1} - \lg r_i) \leq c \cdot \lg r_1 \lg r_0$

$O(\lg r_1 \lg r_0)$

$$\underbrace{\begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}}_{Q_i}\begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}$$

$$r_{i+1} = r_{i-1} - \underline{q_i} r_i$$

$$\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = Q_1 \begin{pmatrix} r_0 \\ r_1 \end{pmatrix} \qquad \begin{pmatrix} r_2 \\ r_3 \end{pmatrix} = Q_2 Q_1 \begin{pmatrix} r_0 \\ r_1 \end{pmatrix}$$

$$\begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix} = \underbrace{Q_k Q_{k-1} \cdots Q_1}_{Q} \begin{pmatrix} r_0 \\ r_1 \end{pmatrix}$$

$$\begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix} = \begin{pmatrix} r_k \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix}\begin{pmatrix} r_0 \\ r_1 \end{pmatrix}$$

$$\boxed{\underbrace{q_{11}}_{\wedge} r_0 + \underbrace{q_{12}}_{\uparrow} r_1 = r_k}$$