The Extended Euclidean Algorithm

$Definition:$ ---

$We\ say\ that\ two\ numbers\ a, b \in \mathbb{Z}\ are\ relativly\ prime\ if\ gcd(a, b) = 1$

$Proprety:$

$if\ a, b \in \mathbb{Z}\ are\ relativly\ prime\ then\ by\ the\ Euclidiant\ Algorithm\ for\ \exists n \in \mathbb{Z}^+,\ r_{n-1} = 1$

$Proof:$

$we\ know\ that\ for\ any\ a, b \in \mathbb{Z}\ Euclidiant\ Algorithm\ after\ n\ iteration\ will\ find\ that$
$d = gcd(a, b) = gcd(r_{n-1}, r_n)\ and\ \ r_n = 0\ (by\ the\ well-ordering\ theorem).\ we\ know\ that\ all$
$iteration\ share\ the\ same\ gcd\ ,\ and\ beause\ a\ and\ b\ are\ relativly\ prime$
$gcd(a, b) = gcd(r_{n-1}, r_n) = gcd(r_{n-1}, 0) = 1,\ hence\ r_{n-1} = 1$

$* \rightarrow\ Algorithm\ for\ finding\ a^{-1}$

$let\ a, b \in \mathbb{Z}\ be\ relativly\ prime\ By\ the\ above\ property\ if\ we\ apply\ the\ Euclidiant\ Algorithm\ we\ will$
$have\ that\ r_{n-1} = 1\ meaning\ that\ r_{n-3} \equiv 1 \bmod r_{n-2},\ because\ r_{n-3} = q_{n-1}*r_{n-2} + r_{n-1},\ now\ i\ will$
$try\ to\ just\ refolmulate\ how\ we\ found\ r_n's\ the\ results\ would\ be\ the\ same$

$algstart:$

$we\ start\ with\ normal\ Euclidean\ Algorithm\ and\ we\ will\ reformulat\ it,$

$$\exists q_1, r_1 \in \mathbb{Z} \times \mathbb{Z}^+\ a = q_1*b + r_1\ \ q_1 = \left\lfloor \frac{a}{b} \right\rfloor\ and\ 0 \leqslant r_1 < b$$

$we\ can\ rewrite\ r_1\ as$

$r_1 = a - q_1 b\ \ = ax_1 + by_1$

$x_1 = 1$

$y_1 = -q_1.$

$if\ r_1 = 0\ then\ b = 1\ and\ a = q_1\ because\ gcd(a, b) = 1$

$else$

$we\ do\ the\ next\ euclidean\ division\ for\ b\ and\ r_1$

$$\exists q_2, r_2 \in \mathbb{Z} \times \mathbb{Z}^+\ b = q_2*r_1 + r_2\ \ q_2 = \left\lfloor \frac{b}{r_1} \right\rfloor\ and\ 0 \leqslant r_2 < r_1$$

$$\begin{aligned} we\ can\ rewrite\ r_2\ as\ r_2 = b - q_2*r_1 &= b - q_2*(a*x_1 + b*y_1) \\ &= b - q_2*a*x_1 - q_2*b*y_1 \\ &= a*(-q_2*x_1) + b*(1 - q_2*y_1) \\ &= ax_2 + by_2 \end{aligned}$$

$x_2 = -q_2 x_1$

$y_2 = 1 - q_2 y_1$

$if\ r_2 = 0\ then\ r_1 = 1\ and\ b = q_2$
$else$
$we\ do\ the\ next\ euclidean\ division\ for\ b\ and\ r_1$

$$\exists q_3, r_3 \in \mathbb{Z} \times \mathbb{Z}^+\ r_1 = q_3 * r_2 + r_3\ \ q_3 = \left\lfloor \frac{r_1}{r_2} \right\rfloor\ and\ 0 \leqslant r_3 < r_2$$

$we\ can\ rewrite\ r_3\ as$

$$\begin{aligned} r_3 = r_1 - q_3 * r_2 &= a*x_1 + b*y_1 - q_3(a*x_2 + b*y_2) \\ &= a*(x_1 - q_3*x_2) + b*(y_1 - q_3*y_2) \\ &= ax_3 + by_3 \end{aligned}$$

$x_3 = x_1 - q_3 x_2$
$y_3 = y_1 - q_3 y_2$
$if\ r_3 = 0\ then\ r_2 = 1\ and\ r_1 = q_2$
$else$
...
$so\ after\ n-1\ iteration\ of\ if\ else\ r_n = 0\ and\ r_{n-1} = 1$

$$\exists q_{n-1}, r_{n-1} \in \mathbb{Z} \times \mathbb{Z}^+\ r_{n-3} = q_{n-1} * r_{n-2} + r_{n-1}\ \ q_{n-1} = \left\lfloor \frac{r_{n-3}}{r_{n-2}} \right\rfloor\ and\ 0 \leqslant r_{n-1} < r_{n-2}$$

$we\ can\ rewrite\ r_{n-1}\ as$

$$\begin{aligned} r_{n-1} &= r_{n-3} - q_{n-1} * r_{n-2} \\ &= ax_{n-1} + by_{n-1} \end{aligned}$$

$x_{n-1} = x_{n-3} - q_{n-1} * x_{n-2}$
$y_{n-1} = y_{n-3} - q_{n-1} y_{n-2}$
$so\ we\ can\ see\ that\ x_{n-1} = x\ and\ y_{n-1} = y\ (because\ r_n = 0),\ so\ we\ found\ r_{n-1} = a*x + b*y\ which$ $implies\ a*x = -b*y + 1,\ we\ did\ found\ x \in \mathbb{Z}\ for\ wich\ a*x \equiv 1 \bmod b\ we\ give\ x\ the\ symbole\ a^{-1}$ $and\ we\ name\ it\ the\ multiplicative\ inverse$
$: endalg$
$for\ a\ clean\ generalisation,\ first\ in\ the\ following\ line\ r_1 = a - q_1 b = ax_1 + by_1\ with\ x_1 = 1\ and$ $y_1 = -q_1,\ we\ see\ here\ that\ x_1\ and\ y_1\ doesn't\ have\ the\ general\ form\ neither\ does\ r_1,\ so\ we\ put$ $r_{-1} = a\ and\ r_0 = b\ wich\ gives\ x_{-1} = 1\ and\ x_0 = 0\ and\ finally\ y_{-1} = 0\ and\ y_0 = 1\ which\ gives\ the$ $following\ initial\ and\ iteration\ condition's$
$r_1 = r_{-1} - q_1 r_0,\ with\ n\ iteration\ r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}\ and\ r_n = 0$
$x_1 = x_{-1} - q_1 x_0,\ with\ n\ iteration\ x_{n-1} = x_{n-3} - q_{n-1} x_{n-2}\ and\ x = x_{n-1}$
$y_1 = y_{-1} - q_1 y_0,\ with\ n\ iteration\ y_{n-1} = y_{n-3} - q_{n-1} y_{n-2}\ and\ y = y_{n-1}$