## Theorem 1.3.4 (The Euclidean Algorithm)

Let $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Then $\exists\, n \geq 1$, $q_2, q_3, \ldots, q_{n+1} \in \mathbb{Z}$, $r_1, r_2, r_3, \ldots, r_n, r_{n+1} \in \mathbb{Z}$ satisfying $r_1 = b$, and

$(a \div b)$ (1) $a = bq_2 + r_2$, $0 < r_2 < b$

$(b \div r_2)$ (2) $b = r_2 q_3 + r_3$, $0 < r_3 < r_2$

$(r_2 \div r_3)$ (3) $r_2 = r_3 q_4 + r_4$, $0 < r_4 < r_3$

$\vdots$

$(r_{n-2} \div r_{n-1})$ $(n-1)$ $r_{n-2} = r_{n-1} q_n + r_n$, $0 < r_n < r_{n-1}$

$(r_{n-1} \div r_n)$ $(n)$ $r_{n-1} = r_n q_{n+1} + r_{n+1}$ $r_{n+1} = 0$.

Furthermore

(i) $r_n = \gcd(a,b)$

(ii) if $c \in \mathbb{Z}$ s.t. $c \mid a$ and $c \mid b$ then $c \mid \gcd(a,b)$

(iii) $\exists\, x, y \in \mathbb{Z}$ s.t. $\gcd(a,b) = xa + yb$.