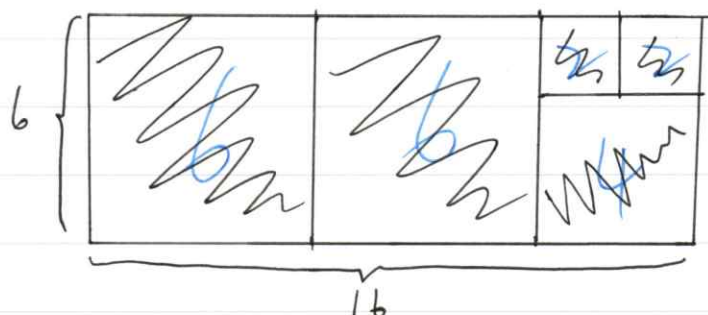


# 欧几里得演算法 辗转相除法 VII

e.g.  $(6, 16) =$



e.g.  $(12921, 4234) = 13$

3	12921 ← 4234 · 3	12921 - 4234 · 3 = 12702
3	4234 ← 12702 · 3	4234 - 12702 · 3 = 161
3	12702 ← 161 · 79	12702 - 161 · 79 = 219
3	161 ← 219 · 0	161 - 219 · 0 = 161
3	219 ← 161 · 1	219 - 161 · 1 = 58
3	161 ← 58 · 2	161 - 58 · 2 = 45
3	58 ← 45 · 1	58 - 45 · 1 = 13
3	45 ← 13 · 3	45 - 13 · 3 = 6
3	13 ← 6 · 2	13 - 6 · 2 = 1
3	6 ← 1 · 6	6 - 1 · 6 = 0

e.g.  $(A, B) \quad A = Bq + R$

⇓

$(A, B) = (B, R)$

$(12921, 4234) = (4234, 219)$

$= (219, 13)$

$= (13, 0)$

$= 13$

Proof.  $A = Bq + R \quad (1)$

$(A, B) = (B, R) \quad (2)$

$\begin{cases} u \rightarrow u \\ v \leftarrow v \end{cases}$

①  $A = a \cdot u, B = b \cdot u$

$R = A - Bq$

$= a \cdot u - b \cdot u \cdot q$

$= u(a - b \cdot q)$

$= n \cdot u$

②  $B = b' \cdot v, R = n' \cdot v$

$A = b'v + n'v$

$= (b' + n')v$

$= a'v$